Facultad de Derecho
Universidad de La Laguna

TRABAJO FIN DE GRADO
Grado en Derecho
Facultad de Derecho
Universidad de La Laguna
Curso 2020/2021
Convocatoria: Julio

LA PROTECCIÓN DE DATOS EN LA UNIÓN EUROPEA Y EL CONSEJO DE EUROPA. ESPECIAL MENCIÓN A LA INCIDENCIA PRODUCIDA POR LA COVID-19.

DATA PROTECTION IN THE EUROPEAN UNION AND THE COUNCIL OF EUROPE. SPECIAL MENTION TO THE INCIDENCE PRODUCED BY COVID-19

Realizado por Claudia Peñas Sáinz.

Tutorizado por la Profesora Dña. Ruth Martinón Quintero.

Departamento: Derecho Público y Privado Especial y Derecho de la Empresa.

Área de conocimiento: Derecho Internacional Público y Relaciones Internacionales

A mis padres, por ser las personas más importantes en mi vida, por apoyarme y quererme de forma incondicional.

ABSTRACT

The main objective of this study is to provide a systematic analysis of data protection in the Eurpean Union and the Council of Europe throughout history by studying its regulations, focusing mainly on Regulation 769/2016 as opposed to the old regulation and noting the main differences and major changes introduced by it.

In addition, the various bodies and institutions responsible for managing and ensuring the correct processing of personal data will be discussed, as well as the proper control of the data in accordance with the principles, duties, powers and obligations to be respected through the tools provided by the data protection regulations, with a special mention of the Data Protection Officer.

Finally, the protection of personal data in the health field will be addressed, especially after the pandemic situation in which we find ourselves having introduced modifications in this field which are currently creating controversy as to where the boundary between the confidentiality of records and the need for information.

Key Words: Protection of personal data, Regulation 678/2016, health field

RESUMEN

El objetivo principal del presente estudio consiste en ofrecer un análisis sistemático de la protección de datos en la Unión Europea a lo largo de la historia, estudiando su normativa, centrando la atención principalmente en el Reglamento 769/2016 en contraposición con la normativa antigua y observando las principales diferencias y los grandes cambios introducidos por el mismo.

Por otro lado, se comentarán los distintos órganos e instituciones encargados de gestionar y garantizar el correcto tratamiento de los datos personales, los cuales son los encargados de mantener el control adecuado de los datos en atención a los principios, deberes, competencias y obligaciones que se deben respetar por medio de las herramientas que proporciona la normativa reguladora de la protección de datos, haciendo una mención especial al Delegado de Protección de Datos.

Por último, se tratará la protección de datos de carácter personal en el ámbito sanitario, especialmente tras la situación de pandemia en la que nos encontramos que ha introducido modificaciones en este campo que actualmente están creando controversia acerca de dónde está el límite entre la confidencialidad de los expedientes y la necesidad de la información por la situación pandémica.

Palabras clave: protección de datos, normativa, Reglamento 679/2016, instituciones, ámbito sanitario.

ÍNDICE

I. INTRODUCCIÓN

El presente trabajo tiene por objeto el análisis jurídico de la protección de datos de carácter personal, su evolución histórica y, en especial, su tratamiento en la Unión Europea. La protección de datos se caracteriza por ser un derecho silencioso, el cual va tomando importancia según va avanzando la tecnología, hasta ser considerado como un derecho fundamental. Es un derecho que va de la mano de otros, principalmente, el derecho a la intimidad y al honor. Actualmente, al encontrarnos en la era digital, donde toda nuestra información está en la red, es fundamental la correcta regulación y protección del derecho a la protección de datos, tanto nacionalmente, cómo a nivel europeo.

La primera aparición de la protección de datos se remonta a la primera Guerra Mundial, donde se usaba como técnica de codificación, pero no es hasta el principio de los años setenta, tras el auge que experimenta la tecnología, dónde aparecen los primeros textos normativos que regulan este derecho.

Teniendo esto como precedente, se va a analizar la normativa más relevante en la materia en Europa, desde el Convenio de 1981 del Consejo de Europa, a la normativa de la Unión Europea: empezando por el Reglamento nº45/2001 del Parlamento Europeo y del Consejo, siguiendo con la Directiva 58/2002/CE del Parlamento Europeo y del Consejo, para finalizar con la normativa actual, que es el Reglamento de la Unión Europea 679/2016.

Asimismo, se estudiarán aquellos órganos e instituciones de la Unión Europea y del Consejo de Europa que tienen un papel relevante en el ejercicio del mantenimiento de los deberes y obligaciones, así como, de garantizar la protección de datos personales por medio del empleo de sus competencias y principios que le son designados por la normativa reguladora de la materia.

Se tratará el tema de la protección de datos en el ámbito sanitario, analizando qué se consideran datos sobre la salud, las especialidades que presenta, y cómo se intenta establecer un equilibrio entre la investigación científica y el interés público. En último

lugar, se estudiará el uso de aplicaciones móviles de rastreo y geolocalización como medios para frenar los contagios producidos por el virus, hasta qué punto estos métodos respetan la privacidad y la protección de datos y cuáles son las medidas que propone la Unión Europea para su control y aplicación.

II. DERECHO DE PROTECCIÓN DE DATOS

1. Antecedentes históricos de la protección de datos.

Durante toda la historia del hombre, se ha venido dando un patrón en referencia a la aparición de las normas, y este es, que estas aparecen con la finalidad de ser el sustento a una necesidad social, es decir, el Derecho es la vía a la que se recurre para solucionar conflictos, ya sean individuales o colectivos. De este modo, y siguiendo esta línea, el derecho a la protección de datos no surge hasta que se percibe que ese derecho puede ser vulnerado o dañado.[1]

La primera aparición del derecho a la protección de datos, se remonta al año 1935 cuando el presidente norteamericano Roosevelt aprueba la *Social Security Act*, una ley que surgió tras la Gran Depresión la cual tenía como objetivo proporcionar una "seguridad social" a través de regular o registrar en primer lugar las pensiones, pero posteriormente se unieron los datos de los trabajadores y posibles incidencias, asistencias médicas, etc…[2] Esta ley propulsó el tratamiento de datos de forma masiva, aunque desgraciadamente, solo pudo cumplir parcialmente los objetivos propuestos debido a la cantidad de datos que se obtuvieron y la falta de material técnico para lidiar con ellos.[3]

Tras ese primer intento de regulación por parte de Estados Unidos, se produjo el impulso técnico definitivo en 1943, cuando un grupo de expertos al servicio británico hicieron tangible su deseo de mejorar y perfeccionar las técnicas de guerra mediante la

[1] REBOLLO DELGADO, L.: *Introducción a la protección de datos*, Ed. Dykinson, Madrid, 2008, Pág 25.
[2] Social Security Act (1935), disponible en https://www.ourdocuments.gov/doc.php?flash=false&doc=68, (fecha de última consulta 13 de abril de 2020)
[3] REBOLLO DELGADO, L.: *op.cit.*, pág 25.

creación del *Colossus,* unos dispositivos calculadores electrónicos cuya finalidad era leer las comunicaciones cifradas alemanas durante la II Guerra Mundial.

En 1967 destacó Alan F. Westin, por su obra "Privacy and Freedom", donde transforma el significado de "the right to privacy", definiéndolo como "la pretensión que tienen los grupos, las personas o las instituciones de determinar por su cuenta, cómo y en qué medida las informaciones que les atañen pueden ser comunicadas a otras personas y, en base a la cual, el individuo debe sentirse libre para decidir por sí mismo qué hechos sobre él se conocen, cuándo y en qué condiciones"[4].

En Europa desde los años sesenta, destaca Vittorio Frosini, el cual entiende que el derecho a la intimidad como una nueva forma de libertad personal, deja de entenderse como la forma de impedir la utilización de informaciones sobre una persona, para entenderse como el control sobre los propios datos personales que salen fuera de la esfera personal para materializarse como elementos de archivo electrónico[5]. Lo que hace Frosini, es entrelazar el derecho a la intimidad con la "libertad informática", entendiendo la segunda como "el derecho de autotutela de la propia identidad informática, es decir, el derecho de controlar los datos personales inscritos en las tarjetas de un programa electrónico"[6]. Es por esto, que el derecho a la intimidad empezó a ser un medio insuficiente para paliar las amenazas y peligros específicos que presentaba el tratamiento automatizado de la información personal, es por ello que en los años setenta se comienza a plantear la creación de un nuevo derecho constitucional[7] (la protección de datos).

La primera norma sobre la protección de datos elaborada en Europa (la Datenschutz) surge en 1970 en el Länder alemán de Hesse, cuya finalidad era limitar el uso de la informática. Posteriormente surgió la Data Lag de Suecia en el año 1973. Estas dos normas nacen a raíz de pretensiones apuntadas por los distintos órganos de la Unión Europea, también destaca la Resolución 509 de la Asamblea del Consejo de Europa, la

[4] WESTIN, ALAN F.: *Privacy and Freedom, Atheneum*, 25 Wash. & Lee L., 1970, pág 368.
[5] GARRIGA DOMÍNGUEZ A.: *Nuevos retos para la protección de datos personales: en la era del Big Data y de la computación ubicua*, Ed. Dykinson, Madrid, 2016, pág 92.
[6] FROSINI, V.: *Informática y Derecho*, Ed. Temis, 1988, pág. 110.
[7] GARRIGA DOMÍNGUEZ A: *op. cit.*, pág 91.

cual trataba el estudio de las tecnologías de la información y su lesividad sobre los derechos de las personas y que tenía como fin poner de manifiesto el conflicto entre los derechos humanos y los logros técnicos[8].

En la evolución de la protección de datos, se pueden diferenciar cuatro generaciones, que a su vez se dividen en dos ramas, la primera, se centra en la evolución de la tecnología y los ordenadores, y la segunda, que es en la que nos vamos a centrar, contempla los cambios que se van produciendo en la forma de entender y regular el derecho a la protección de datos[9].

La primera generación de normas sobre la protección de datos abarca la protección sobre el espacio físico en que se ubica la información, es decir, incluye tanto al propio ordenador, cómo a la base de datos. Esto es así, porque en esta etapa la Administración pública era quien manejaba las bases de datos, por lo que el foco está en crear autorización para el acceso y uso de esos datos. También se crean instituciones que tenían como fin el control del tratamiento de los datos, elaborando informes que debían remitir al parlamento. Las normas más características de esta primera generación fueron, la Datenschutz, la Data Lag y la Landesdatenschutzgesetz del Länd de Renania-Palatinado.[10]

La segunda generación mantiene el objetivo de conservar la calidad de los datos, pero, además, se empieza a entender lo peligroso o lesivo que puede ser el uso de la informática, es por este motivo que se incluye por primera vez el término de lesión de los derechos, fundamentado en una mala utilización de los datos. En esta etapa, nacen los principios básicos del tratamiento de datos (el consentimiento del titular, el derecho de acceso y control y la obligación de mantener la calidad de los datos), y a la vez, también aparece el concepto de datos sensibles, en este nuevo grupo de datos se incluye el sexo, la raza, la religión, ideologías políticas etc… es decir, aquellos datos más personales e identificativos de las personas.

[8] REBOLLO DELGADO, L.: *Introducción a la protección de datos*, Ed. Dykinson, Madrid, 2008, Págs 27-28
[9] *Idem*, pág 30
[10] *Idem*, pág 31.

La norma que mayor importancia tuvo en este periodo fue la ley francesa de 6 de enero de 1978 relativa a la informática, archivos y libertades. Lo destacable de esta norma fue que, en solo 45 artículos, supo reflejar el problema de la relación informática y los derechos fundamentales tanto en lo personal o individual como en lo colectivo.[11]

La tercera generación no destaca por la creación de nueva normativa, sino por ser el inicio del camino para la consagración del derecho a la autodeterminación informática como un derecho autónomo. La sentencia de 15 de diciembre de 1983 del Tribunal Constitucional Federal Alemán reconoce por primera vez el derecho a la autodeterminación informativa entendiéndola como la facultad general de disponer de datos propios[12]. Según Erhand Denninger (un destacado catedrático de Derecho Público en la Universidad de Frankfort), lo destacable de esta sentencia es que da a entender que "la autodeterminación informativa no solo depende de los datos sino de su elaboración, es decir, el peligro para el derecho a la autodeterminación de las personas no se encuentra en el carácter del dato más o menos íntimo, tampoco importa que el dato tenga, o no, carácter secreto, "lo que importa es su utilidad y la posibilidad de su aplicación"[13].

Por lo tanto, la Sentencia de 15 de diciembre de 1983 determina que la idea clave es "saber la finalidad con la cual se reclaman los datos y que posibilidades de interconexión y de utilización existen, porque una vez determinado esto, se podrá contestar la interrogante sobre la licitud de las restricciones del derecho a la autodeterminación informativa"[14].

A nivel nacional destaca el trabajo de Antonio Enrique Pérez-Luño, ya que fue el pionero en estudiar la situación de erosión y degradación de los derechos fundamentales por determinados usos de las nuevas tecnologías y el uso del derecho a la autodeterminación informativa cuya protección la establece por el denominado habeas

[11] *Idem*, pág 32.
[12] GARRIGA DOMÍNGUEZ A.: *Nuevos retos para la protección de datos personales: en la era del Big Data y de la computación ubicua*, Ed. Dykinson, Madrid, 2016, pág 93.
[13] DENNINGER, E.: *El derecho a la autodeterminación informativa*, en PÉREZ LUÑO, Anto- nio E.: *Problemas actuales de documentación y la informática jurídica*, Tecnos Madrid, 1987, p. 273.
[14] Sentencia del Tribunal Constitucional Alemán de 15 de diciembre de 1983.

data o habeas scriptum, que aparece como[15] "la facultad de las personas de conocer y controlar las informaciones que les conciernen procesadas en bancos de datos informatizados, frente a los nuevos fenómenos abusivos que limitan la esfera informática de la libertad de la persona"[16].

En último lugar, la cuarta generación gira en torno a la necesidad de crear una legislación a nivel supranacional por parte de la Unión Europea que ayude a unificar la disparidad normativa que tenían los Estados Miembros en ese momento, de ahí nace la Directiva 95/46/CE la cual tiene un periodo de vida de dos años, al ser sustituida por la Directiva 97/66/CE que disponía de un carácter mucho más genérico y con mayor enfoque en las telecomunicaciones, obligando a los Estados Miembros a establecer normas que garantizaran la confidencialidad de las comunicaciones por medio de las redes públicas.[17]

Con el uso de estas directivas, lo que pretendía conseguir la Unión Europea era equilibrar la protección de las libertades y derechos fundamentales, especialmente en derecho a la intimidad. En España estas dos directivas provocaron que la ley de 1992 fuera modificada por la actual Ley Orgánica 15/1999.[18]

2. Concepto y fundamentación de la Protección de Datos.

El fundamento de la protección de datos no puede entenderse sin la conexión con el derecho a la intimidad, ya que los ordenamientos jurídicos centran la protección de los derechos de los ciudadanos frente a la informática o cualquier ingenio informático a través de él, por lo que el derecho a la intimidad puede contemplarse en tres concepciones[19]:

a) El concepto objetivo del derecho a la intimidad.

[15] GARRIGA DOMÍNGUEZ A: *op. cit.*, pág 92.
[16] PÉREZ LUÑO, ANTONIO E.: "*Del habeas corpus al habeas data",* en Informática y Derecho, nº 1, UNED, Centro Regional de Extremadura, Mérida, 1992, p. 156.
[17] REBOLLO DELGADO, L.: *Introducción a la protección de datos*, Ed. Dykinson, Madrid, 2008, pág 34.
[18] *Ibidem.*
[19] *Idem* pág 35.

Se basa en la teoría de las esferas o de los círculos concéntricos de la doctrina alemana, la cual establece que el núcleo, el círculo más pequeño se corresponde con lo íntimo, la siguiente esfera en tamaño se correspondería con lo familiar, en la siguiente se encontraría el secreto o cuestiones confidenciales, y, por último, el círculo más grande o el primero sería la esfera pública. Esta teoría menciona estas esferas o niveles, pero no son conceptos cerrados, ya que cada individuo puede configurar los mismos en la forma que mejor le convenga[20]. Este concepto es el que usa nuestro Tribunal Constitucional cuando establece que *"*la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de vida humana[21]. *"*

Cabe destacar, que este concepto se corresponde con la protección de un ámbito concreto del individuo, es decir se entiende el concepto de intimidad como un derecho de defensa.[22]

b) El concepto subjetivo del derecho a la intimidad.

Este concepto se corresponde con el derecho a la autodeterminación informativa, la cual se basa en la Sentencia del Tribunal Constitucional alemán de 1983 comentada anteriormente. Nuestro Tribunal Constitucional por otro lado, se ha acogido al uso de esta concepción en muchas ocasiones, al asegurar que el derecho a la intimidad es[23] "la aptitud de exclusión de los demás, de abstención de injerencias por parte de otros en la vida privada y personal salvo consentimiento del individuo."[24]

Este concepto, a diferencia del objetivo, tiene como trasfondo la libertad, es decir no es solo la defensa del mismo, sino que el individuo puede controlar aquello que es externo a él, pero le va a afectar.[25]

c) Teoría del mosaico.

[20] *Ibidem*.
[21] Sentencia del Tribunal Constitucional de 2 de diciembre de 1988 (rec. núm. 1247/1986).
[22]REBOLLO DELGADO, L: *op. cit.*, pág 36.
[23] *Idem*, pág 37.
[24] Sentencia del Tribunal Constitucional, de 15 de noviembre de 2004 (rec. núm.1322/2000).
[25]REBOLLO DELGADO, L: *op. cit*, pág 37.

Esta teoría es creada por Madrid Conesa, quien entiende "que la teoría de las esferas ya no es válida debido a que los conceptos de lo que podría considerarse como privado o público no tienen una delimitación clara y, por lo tanto, esta separación a nivel práctico presenta más dificultades que beneficios"[26].

Actualmente, la concepción de intimidad que se ajusta más a las necesidades de nuestro ordenamiento jurídico sería una mezcla entre el concepto objetivo y subjetivo, ya que fusionan el derecho a la defensa del mismo, junto con al control que puede hacer el individuo sobre él[27].

El derecho a la intimidad se engloba como un espacio restringido donde el individuo tiene total libertad, aunque para que pueda desarrollarse de forma completa debe de tener relación con otros individuos, hacerse valer frente a ellos o incluso compartirse. Por esta razón, este derecho no es un concepto cerrado, sino que va a depender del componente subjetivo de cada persona, teniendo elementos determinantes como pueden ser su edad, cultura y sociedad, entre otros.[28]

Por lo que teniendo en consideración todo lo dicho hasta ahora, podemos determinar, que el derecho a la intimidad se corresponde con la autorrealización del individuo, en otras palabras, es el derecho que disponen los individuos de que ciertos ámbitos de su vida se mantengan desconocidos para los terceros, al igual que el poder de controlar que pueden o no saber estos, por lo que el derecho a la intimidad se puede asumir como una desconexión social[29]. Como afirmaba Frosini, "los ordenamientos jurídicos han optado por dos posturas: "una seguida por la legislación americana que se concreta en el principio de que todo está permitido, salvo lo que está prohibido, y otra cuyo representante principal es Alemania, la cual entiende que cualquier actividad relativa al procesamiento de datos personales está prohibida, salvo cuando está permitida"[30].

[26] MADRID CONESA, F: *Derecho a la intimidad, informática y Estado de Derecho*. Universidad de Valencia. Valencia 1984, pág. 45.
[27] REBOLLO DELGADO, L: *op. cit*, pág 38.
[28] *Ibidem*.
[29] Idem pág 39
[30] FROSINI, V: *Bases de datos y tutela de la persona*. Revista de Estudios Políticos (NE) nº 30 de 1982, pág. 30.

Viendo estas dos posturas, podemos decir que tanto el ordenamiento jurídico europeo como el español, se encuentran dentro de esta segunda postura.[31]

Con este pequeño análisis del derecho a la intimidad, se refleja claramente su relación con el derecho a la protección de datos, el cual protege tanto a la dignidad humana como a un ámbito de la libertad del individuo[32].

La protección de datos es un derecho fundamental que tiene unos rasgos característicos basados en la definición constitucional, que establecen que el individuo tiene el derecho de consentir sobre la utilización y recolección de sus datos personales, al igual que a controlar quien es conocedor de los mismos. Se puede concretar, que la protección de datos personales es la protección jurídica sobre el tratamiento de sus datos de carácter personal, restringiendo la utilización de estos por terceros de forma no autorizada para evitar lesiones en su entorno personal, social o profesional, manteniendo los límites del derecho a la intimidad[33].

El estudio de la protección de datos personales establece tres características:

- Los datos deben ser susceptibles de tratamiento o que se encuentren en un soporte que sea susceptible de tratamiento.
- Que tenga la posibilidad de identificar el resultado de los datos con su titular.
- Que el manejo o acceso de los datos se produzca sin el consentimiento del titular.

El estudio de la protección de datos se centra en la incidencia de los datos en relación con la defensa del bien jurídico protegido y los intereses que se pueden ver afectados como consecuencia de una manipulación de los mismos. Hay que tener en cuenta que, el tratamiento informático de los datos ha traído consigo múltiples ventajas y facilidades a nuestra vida cotidiana, pero también al manejar tanta información que en la mayoría de casos tiene carácter personal o privado, es necesario exigir una seguridad física en

[31] REBOLLO DELGADO, L: *op. cit*, pág 39.
[32] *Idem*, pág 40.
[33] CONDE ORTIZ, C.: *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad*, Ed. Dykinson, Madrid, 2006, pág 29.

los sistemas informáticos y de comunicaciones, con el fin de evitar lesiones en los derechos fundamentales de los individuos.[34]

El derecho a la intimidad informática, como sucede con todos los derechos fundamentales debe estar reconocido y limitado por nuestra Constitución, en esta también se encuentran unas limitaciones que el Tribunal Constitucional reconoce frente al derecho a la intimidad, algunas de ellas indirectas, producidas por las obligaciones que el texto constitucional le adjudica a los poderes públicos y a los particulares[35]. En ella se argumenta que "todo derecho tiene sus límites que con relación a los derechos fundamentales establece la Constitución, por sí misma, en algunas ocasiones, mientras el otro límite deriva de una manera mediata o indirecta de tal norma en cuanto ha de justificarse por la necesidad de proteger y observar otros derechos constitucionales, sino también otros bienes constitucionales protegidos".[36]

En España el concepto de intimidad se asocia a una parte restringida de nuestra vida, lo que la Unión Europea denomina como vida privada. En nuestro país estos dos conceptos se usan indistintamente ya que su significado es prácticamente el mismo, en cambio en la Unión Europea el concepto de vida privada tiene un significado más amplio, y dentro de este, se localiza la intimidad.[37]

Durante los años, distintos autores han coincidido en que la intimidad se puede abordar desde tres perspectivas distintas, en primer lugar, como *derecho*, donde se entiende que esta intimidad es la manifestación y reconocimiento jurídico de una necesidad social, en segundo lugar, como *fenómeno*, esto se refiere a la necesidad universal de los individuos a tener intimidad, y, por último, como *idea*, es decir, la forma de conciencia sobre la intimidad de las distintas sociedades.[38]

[34] I*bidem.*
[35] *Idem*, pág 30.
[36] FREIXAS GUTIERREZ, G.: *La protección de los datos de carácter personal en el derecho español,* Bosh, Barcelona, 2001, pág 40-41
[37] REBOLLO DELGADO, L.: *Protección de datos en Europa: origen, evolución y regulación actual*, Ed. Dykinson, Madrid, 2018, pág 24.
[38] *Idem*, pág 25.

3. Derecho a la autodeterminación informática.

Los derechos humanos según reflexionaba PÉREZ-LUÑO, "son un catálogo permeable y abierto a la incorporación de nuevos valores y nuevos derechos. Procederá en consecuencia, efectuar una reformulación de los derechos fundamentales reconocidos, así como ampliar el catálogo de los existentes, si con dicho reconocimiento no se ofreciere respuestas a las nuevas demandas individuales derivadas de una sociedad informatizada y en continuo progreso"[39].

Considerando entonces, que los derechos fundamentales no son conceptos fijos, a lo largo de la historia, los juristas identifican tres generaciones, donde en cada una de ellas, se plasma un momento ideológico y social diferentes, por lo que introducían importantes rasgos de diferenciación y equivalencia entre los derechos que se adscribían en cada una de ellas.

Actualmente, nos encontramos ante la Tercera Generación, la cual tiene el objetivo de complementar la protección que el individuo necesita, propias de la era tecnológica. También, se han creado nuevos derechos fundamentales, cómo, el de la protección de datos, la protección del medioambiente, entre otros. La inclusión de estos, implica que obtienen significación propia, y su diferenciación tiene como fundamento:

- *La naturaleza jurídica:*

Esta se centra en adquirir el significado propio de la sociedad actual, en la que predominan las relaciones entre individuos y la tecnología informática.

- *Su razón de ser*

La solidaridad es el valor que tiene esta generación como referencia.

- *El elemento subjetivo***.**

Es la defensa y tutela de estos derechos, se pretende ampliar la legitimación para la protección de los mismos frente a la totalidad de individuos, ya que estamos ante derechos cuyos bienes jurídicos son difusos.

[39] PÉREZ-LUÑO, A.: "Nuevos derechos fundamentales de la era tecnológica: la libertad informática", *ADPEP*, núm.2 1989/90, pág 176.

Los derechos que aparecen en la Tercera Generación son: el derecho al medio ambiente sano, defensa de los consumidores o usuarios, pero el que destaca entre ellos, es el derecho a la libertad informática o autodeterminación informativa[40].

El Tribunal Constitucional observa la importancia de configurar la libertad informática junto con el análisis de la intimidad en la sociedad contemporánea, esto se ve reflejado en la Sentencia del Tribunal Constitucional 110/84, en la cual se deja ver como el Tribunal propone un reconocimiento global de un derecho a la intimidad o a la vida privada que abarque las intromisiones que por cualquier medio puedan realizarse en ese ámbito reservado de la vida privada.[41]

Esta sentencia muestra las preocupaciones del Alto Tribunal por el tratamiento automatizado de los datos y la intromisión en la vida social de los avances técnicos e informáticos. La razón de esta preocupación es la amenaza que las nuevas tecnologías suponen para la garantía y el respeto de los derechos individuales y de la personalidad.

Libertad informática como derecho fundamental

La Sentencia del Tribunal Constitucional 254/93, de 20 de julio, introduce la idea de la incorporación a nuestra Constitución de una nueva garantía constitucional, "como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona. En el presente caso, estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto, qué es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona proveniente de un uso ilegitimo del tratamiento mecanizado de datos, lo que la Constitución llama la informática"[42].

El contenido a la intimidad y protección de datos

[40] ORTIZ HERRÁN, ISABEL A.: *El Derecho a la Intimidad en la nueva Ley Orgánica de Protección de Datos Personales*, Ed. Dykinson, Madrid, 2002, págs. 54-57.
[41] *Idem*, págs 107
[42] STC 254/93, de 20 de julio (rec. núm. 1827/1990)

En la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, se esclarecen los límites que separan al derecho de la intimidad frente al derecho de la libertad informática. Esto queda reflejado en su fundamento jurídico quinto donde plantea que " este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art 18.1 Constitución Española, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consisten en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme el artículo 18.4 Constitución Española debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art.18.1 Constitución Española), bien regulando su ejercicio. La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues en su distinta función, lo que apareja que también su objeto y contenido difieran"[43].

El Tribunal lleva a cabo una diferenciación entre las funciones de los derechos mencionados, en primer lugar, la función del derecho fundamental a la intimidad es la protección de la vida personal y familiar frente a cualquier ataque, por otro lado, la función del derecho fundamental a la protección de datos es garantizar a la persona el control sobre sus datos personales.

Esta continua diferenciación lo que hace es de limitar el objeto de protección de datos del derecho fundamental a la libertad informática, en este sentido, se entiende que esta libertad informática no se basa en los datos íntimos de la persona, sino que abarca a cualquier dato personal, sea intimo o no, siempre que la utilización o conocimiento de los mismos pueda afectar a los derechos y libertades de la persona. Se aclara también que su alcance es tanto para los datos de carácter personal como para los datos personales públicos.[44]

[43] STC 292/2000, de 30 de noviembre (rec. núm 463/2000)
[44]ORTIZ HERRÁN, ISABEL A, *op.cit*, págs 108-110.

4. El Consejo de Europa.

El Consejo de Europa es una organización intergubernamental que fue fundada por el Tratado de Londres de 5 de mayo de 1949, de la cual forman parte 47 Estados europeos. Tiene su sede en Estrasburgo, Francia[45].

La finalidad del Consejo de Europa según el Tratado de Londres es "realizar una unión más estrecha entre sus miembros para salvaguardar y promover los ideales y los principios que constituyen su patrimonio común y favorecer su progreso económico y social[46]".

Para poder llevar a efecto su objetivo, utiliza varios mecanismos, cómo por ejemplo, la conclusión de acuerdos, adopción de acciones (económicas, sociales, culturales, jurídicos, etc…), y la más importante, la salvaguarda de los derechos humanos y las libertades fundamentales. El respeto a los Derechos Humanos, la Democracia y el Estado de Derecho, se garantizan y protegen por medio de un amplio abanico de tratados internacionales y por la cooperación intergubernamental[47].

En materia de protección de datos del Consejo de Europa podemos destacar su normativa, cómo sus instituciones:

1. Normativa.

El convenio de 1981 del Consejo de Europa

Este Convenio es la primera norma del Consejo de Europa relativa a la protección de datos. Destaca por la regulación de la protección de datos a través de una serie de principios básicos, al igual que establece criterios y la creación de un Comité Consultivo encargado de proponer mejoras relativas a la aplicabilidad del mismo. El Convenio de 1981 establece el marco genérico de protección de las personas frente a las intromisiones en su intimidad, o la lesión de derechos por parte de la informática, por lo que para garantizar una mayor protección y regulación es necesario la creación o desarrollo de otra normativa tanto a nivel europeo como nacional[48].

[45]Disponible en http://www.exteriores.gob.es (fecha de última consulta: 26 de junio de 2021)
[46] Tratado de Londres de 5 de mayo de 1949.
[47] Disponible en http://www.exteriores.gob.es (fecha de última consulta: 26 de junio de 2021)
[48] GARRIGA DOMÍNGUEZ, A.: *Nuevos retos para la protección de datos personales: en la era del Big Data y de la computación ubicua*, Ed. Dykinson, Madrid, 2016, pág 151.

Este Convenio establece una serie de principios para la protección de datos, estos, tienen carácter imperativo para aquellos Estados que hayan ratificado el Convenio. Dentro del principio de calidad de los datos se encuentran a su vez los siguientes principios:

a. Principio finalista. Dentro de este a su vez podemos encontrar el principio de utilización no abusiva, el principio del derecho al olvido y la pertinencia de los datos.
b. Principio de lealtad.
c. Principio de exactitud y veracidad.
d. Principio de publicidad.
e. Principio de acceso individual.
f. Principio de seguridad.
g. Principio de finalidad.
h. Principio de pertenencia.
i. Principio de limitación temporal.

Los principios y los derechos que se encuentran en este Convenio no tienen el carácter de absolutos, esto quiere decir, que se pueden limitar cuando sea necesario, como por ejemplo, en la protección de la seguridad del Estado, la seguridad pública, etc…[49]

El Convenio produce la armonización del Derecho interno de los Estados Miembros en estas materias, pero también constituye "el primer paso importante en la elaboración de un armazón legislativo común[50]". Un rasgo muy característico de este Convenio, es que le da prioridad a la garantía de la libre circulación de los datos personales entre los pueblos, sin importar las fronteras, pero en su artículo 12.3 se contempla, en primer lugar, la posibilidad de la no exportación de datos personales cuando el destinatario sea un estado no contratante, y, en segundo lugar, tampoco se contempla la exportación cuando la legislación interna de un Estado Miembro estipule una protección especial, y el país de destino no cuente con una protección equivalente[51].

[49] Ibidem
[50] CAMPUZANO TOMÉ, Herminia: *Vida privada y datos personales*, Tecnos, Madrid, 2000, p. 79.
[51] GARRIGA DOMINGUEZ, A. *op.cit*, pág 151

Por último, este Convenio "presenta importantes debilidades en su aplicación, por una parte, al permitir que los Estados parte desarrollaran el contenido de los principios y, por otra, al dar libertad para aplicar las excepciones con lo que podría ocurrir que los datos personales protegidos por el Convenio no lo estén en el Estado adherido, si así lo recoge expresamente en el instrumento de ratificación[52].

2. Instituciones.

El Comisario para los Derechos Humanos

Es creado por el Consejo de Europa mediante Resolución del Comité de Ministros el 7 de mayo de 1999. Promover la educación y sensibilización de las personas en materia de protección de los derechos fundamentales, así como el cumplimiento de las normas del Consejo de Europa, es su principal función[53].

Al no disponer de un carácter judicial, está abierto a recibir quejas de los particulares, y como expresa Arenas Ramiro: "desarrolla un papel complementario de las demás instituciones, es decir, se encuentra en una posición intermedia entre los órganos de asistencia técnica y los órganos de mediación[54]."

Respecto a la protección de datos de carácter personal, destaca la imposibilidad de recibir quejas por parte de los ciudadanos relativas al art.8 del CEDH, ya que en esta materia su actividad se centra en la emisión de informes, debido a su carácter asesor y preventivo[55].

Agencia de los Derechos Fundamentales de la Unión Europea

Esta Agencia se crea en virtud del Reglamento nº 168/2007 del Consejo de 15 de febrero de 2007. Su objetivo principal, es la lucha contra el racismo, la xenofobia y la intolerancia, en consonancia con esto, el art.5 del Reglamento citado, establece que

[52] ARENAS RAMIRO, M.: *El derecho fundamental a la protección de datos personales en Europa*, Ed. Tirant lo Blach, Valencia, 2006, pág. 156.
[53] *Idem*, pág 183
[54] ARENAS RAMIRO, M.: *El derecho fundamental a la protección de datos personales en Europa*, Ed. Tirant lo Blach, Valencia, 2006, pág 182
[55] REBOLLO DELGADO, L, *op. cit*., pág 183

también tiene como finalidad el aumento de la sensibilización en la opinión pública en lo referente a los derechos fundamentales[56].

III. REGULACIÓN JURÍDICA DEL DERECHO A LA PROTECCIÓN DE DATOS EN LA UNIÓN EUROPEA.

1. La regulación de la normativa europea sobre la protección de datos a lo largo del tiempo.

Para llevar a cabo el correcto análisis de la protección de datos de carácter personal en Europa, es necesario el estudio tanto de la normativa vigente como de la evolución de la misma, para comprender el camino que se ha recorrido hasta conseguir la normativa actual de la materia. La protección de datos pasa a formar parte del Derecho comunitario originario en 1997 tras las reformas introducidas por el Tratado de Ámsterdam en el Tratado de la Comunidad Europea (en particular, el artículo 286)[57].

La Carta de Derechos Fundamentales de la Unión Europea proclamada en Niza en el año 2000, y jurídicamente vinculante desde la entrada en vigor del Tratado de Lisboa (por el artículo 6 del Tratado de la Unión Europea), incluye dentro de su catálogo de derechos fundamentales (concretamente en su artículo 8), el derecho de la protección de datos. Lo característico de la Carta, es que, reconoce tanto el derecho al respeto a la vida privada y familiar, cómo el derecho a la protección de datos personales como derecho autónomo e independiente del anterior[58].

La decisión de reconocer este derecho como autónomo se debe al entender que es necesario garantizar una tutela específica para la recogida y el almacenamiento de información sobre las personas, ya que esta actividad puede suponer un peligro para otros derechos fundamentales, es especial, la privacidad[59].

---

[56] REBOLLO DELGADO, L.: *Protección de datos en Europa: origen, evolución y regulación actual*, Ed. Dykinson, Madrid, 2018, pág 187
[57] RAMIRO ARENAS, M.: *El Derecho fundamental a la protección de datos personales en Europa*, Ed. Tirant lo Blanch, Valencia, 2006, pág 235.
[58] *Idem*, pág 236.
[59] *Idem*. Pág 245.

Evolución de la Normativa Europea en materia de protección de datos:

1. *Reglamento nº45/2001 del Parlamento Europeo y del Consejo de la Unión Europea.*

Según su Considerando 12, este Reglamento, surge con la finalidad de que "se garantice en toda la Comunidad Europea una aplicación coherente y homogénea de las libertades fundamentales de las personas en lo que respecta al tratamiento de datos personales[60]", al igual que también busca el respeto de la normativa sobre la libre circulación de los datos personales entre los Estados Miembros y las instituciones u organismos comunitarios[61].

Los destinatarios del Reglamento nº45/2001 de la Unión Europea, son las instituciones de la Unión Europea, ya que era necesario disponer de una normativa que tratara el sometimiento de las mismas a la protección de datos y la libre circulación de los mismos. Este Reglamento crea dos figuras, la primera se corresponde con la Autoridad de Control con carácter independiente, cuya función es la vigilancia de los tratamientos de los datos personales llevados a cabo por las distintas instituciones y organismos comunitarios. En segundo lugar, encontramos el Supervisor Europeo para la Protección de Datos de carácter personal[62].

Lo que resalta de este Reglamento es la tabla de derechos que establece, haciendo una diferencia entre aquellos derechos que concurren cuando es el propio interesado el que recaba la información y cuando no es así. El art.11 regula el primer caso, mientras que el art 12 recoge aquellos datos que no han sido recabados por el interesado.

Los derechos que establece tras haber explicado la división que hacen son los siguientes:

a. Derecho de acceso (art 13)
b. Derecho de rectificación (art 14)

[60] Reglamento (CE) nº 45/2001 del Parlamento Europeo y de Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.
[61] REBOLLO, L.*: Protección de datos en Europa, origen, evolución y regulación actual*, Ed. Dykinson 2018, pág 85.
[62] *Idem*, pág 87.

c. Derecho de bloqueo (art 15)
d. Derecho de supresión (art 16)
e. Obligación de notificación a terceros (art 17)
f. Derecho de oposición del interesado
g. Decisiones individuales automatizadas (art 19)
h. Derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado (art 22)

Por último, es necesario comentar los criterios necesarios para la licitud del tratamiento de los datos, los cuales vienen regulados en el art 5 y 6 del Reglamento.
El artículo 5 establece cuando podrá efectuarse el tratamiento de datos, y lo hace de la siguiente forma[63]:

- "a) es necesario para el cumplimiento de una misión de interés público en virtud de los Tratados constitutivos de las Comunidades Europeas o de otros actos legislativos adoptados sobre la base de los mismos o es inherente al ejercicio legítimo del poder público conferido a la institución o al organismo comunitario o a un tercero a quien se comuniquen los datos
- b) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento.
- c) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado
- d) el interesado ha dado su consentimiento de forma inequívoca.
- e) es necesario para proteger los intereses esenciales del interesado."[64]

El artículo 6 por otro lado, hace referencia a aquellas situaciones en las cuales los datos podrán ser tratados de forma distinta a lo establecido en los artículos 4, 5 y 10, en primer lugar, cuando así se prevea en una norma interna o del organismo comunitario,

[63] *Idem*, págs. 88, 89, 90, 91 y 92.
[64] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016

y, en segundo lugar, que su fin sea la prevención, la investigación, la detención o la represión de acciones penales graves[65].

2. Directivas sobre la Protección de Datos Personales.

a. La Directiva 95/46/CE sobre Protección de Datos Personales.

Esta Directiva tiene un doble objetivo, en primer lugar, aumentar el nivel de protección dentro de toda la Comunidad Europea a través de garantizar el derecho a la vida privada (especialmente en lo referente al tratamiento de datos personales) establecido en el artículo 8 del CEDH. En segundo lugar, impedir la restricción de la libre circulación de los datos personales por medio de la aplicación de los mismos principios relativos al tratamiento de datos personales en todos los Estados Miembros de la Unión Europea[66].

Pero para poder obtener una regulación común y flexible, hay que tener en cuenta tanto el estado de la tecnología como la capacidad y el desarrollo técnico de cada Estado Miembro. Por lo que solo se puede asegurar una normativa eficaz, si la misma cuenta con reglas flexibles y en continua actualización[67].

Según parte de la doctrina, esta Directiva se asemeja más a una norma habilitante para los operadores que a una norma protectora[68].

b. La Directiva 2002/58/CE sobre Protección de Datos y Comunicaciones Electrónicas

Esta directiva se enfoca en el tratamiento de datos personales y la protección de la intimidad en el sector de las comunicaciones electrónicas en todos los Estados Miembros, además introdujo en este campo especificaciones propias de las telecomunicaciones en los datos personales. La causa de su desarrollo fue que la anterior Directiva, la 97/66 de 15 de diciembre se quedó envejecida debido al avance de

[65] REBOLLO, L.: *Op cit.*, págs. 93 y 94.
[66] ARENAS RAMIRO, M.: *El derecho fundamental a la protección de datos personales en Europa*, Ed. Tirant lo Blach, Valencia, 2006, pág 277.
[67] *Idem*, pág 278.
[68] *Ibidem*.

la tecnología. La trasposición de la misma en el ordenamiento jurídico español se corresponde con la Ley 32/2003 de 3 de noviembre[69].

Su finalidad era la de eliminar el envío de correos conocido comúnmente como "spam", es decir correos que se suelen identificar con publicidad de servicios o productos, de este modo, se buscaba la seguridad y confidencialidad en lo relativo al mundo de internet en la Unión Europea, El objetivo más destacable de la Directiva es el tratar de impedir que la identidad de los remitentes de correos spam se camufle debido a la utilización de direcciones falsas, al igual que prevé el control de la instalación de cookies (archivos que se instalan en el ordenador del usuario al conectarse a una página web), o programas spyware (utilizados para recoger información de los usuarios en internet) sin el consentimiento del usuario[70].

En lo referente a su articulado, los artículos más destacables son los artículos 5 y 6. El primero regula la confidencialidad de las comunicaciones, mientras que el segundo, establece obligaciones relativas a los datos de tráfico[71].

c. Otras Directivas.

En la Unión Europea, aparte de las Directivas mencionadas, se han creado muchas otras dónde a pesar de que la protección de datos no es el objeto principal de las mismas, si que afectan en cierto modo de forma directa a esta materia. Algunos ejemplos de estas directivas serían[72]:

- La Directiva sobre Protección de Bases de Datos[73]
- La Directiva sobre Protección de Consumidores en Contratos a Distancia[74]
- La Directiva sobre Firma Electrónica[75]

[69] REBOLLO, L.: *Protección de datos en Europa, origen, evolución y regulación actual*, Ed. Dykinson 2018, pág 94.
[70] *Idem*, pág 95.
[71] *Ibidem*.
[72] ARENAS RAMIRO, M.: *El derecho fundamental a la protección de datos personales en Europa*, Ed. Tirant lo Blach, Valencia, 2006, pág 282.
[73] Directiva 96/9/CE, de 11 de marzo, del Parlamento Europeo y del Consejo, sobre la protección jurídica de las bases de datos.
[74] Directiva 97/7/CE, de 20 de mayo, del Parlamento Europeo y del Consejo, relativa a la protección de consumidores en materia de contratos a distancia
[75] Directiva 1999/93/CE, de 13 de diciembre, del Parlamento Europeo y del Consejo, por la que se establece un marco comunitario para la firma electrónica

- La Directiva sobre Comercio Electrónico[76]
- La Directiva de Acceso a Redes de Comunicaciones Electrónicas[77]
- La Directiva de Autorización de Redes de Comunicación Electrónicas[78]
- La Directiva del Marco Regulador de las Redes y Servicios de Comunicaciones Electrónicas[79]
- La Directiva de Servicio Universal de Comunicaciones Electrónicas[80]
- La Directiva sobre la obligación de los transportistas de comunicar datos de las personas transportadas[81]

3. Otra Normativa.

Toda la normativa tratada hasta ahora es lo que compone al régimen general en materia de protección de datos en la Unión Europea, pero también se encuentran otros instrumentos específicos en la materia. En primer lugar, se encuentran unos organismos dentro de la Unión Europea con funciones específicas dentro del ámbito comunitario y que entablan una estrecha relación con los datos personales, estos organismos son: el Sistema para la comparación de huellas dactilares (Eurodac), el Sistema de Información de Visados (VIS) y la Oficina Europea Estadística (Eurostat)[82].

En segundo lugar, la Directiva 95/46/CE sobre Protección de Datos Personales establece "que quedan fuera de su ámbito de aplicación los tratamientos de datos personales que se efectúen al margen del derecho Comunitario[83]", es decir, está haciendo referencia al tratamiento de los datos personales en materia de política exterior

[76] Directiva 2000/31/CE, de 8 de junio, del Parlamento Europeo y del Consejo, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior.
[77] Directiva 2002/19/CE, de 7 de marzo, del Parlamento Europeo y del Consejo, relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión
[78] Directiva 2002/20/CE, de 7 de marzo, del Parlamento Europeo y del Consejo, relativa a la autorización de redes y servicios de comunicaciones electrónicas
[79] Directiva 2002/21/CE, de 7 de marzo, del Parlamento Europeo y del Consejo, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas
[80] Directiva 2002/22/CE, de 7 de marzo, del Parlamento Europeo y del Consejo, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas
[81] Directiva 2004/82/CE, de 29 de abril, del Parlamento Europeo y del Consejo, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas
[82] ARENAS RAMIRO, M.: *El derecho fundamental a la protección de datos personales en Europa*, Ed. Tirant lo Blach, Valencia, 2006, pág 284.
[83] Directiva 95/46/CE sobre Protección de Datos Personales (artículo 3.2)

y seguridad común, y en materia de cooperación policial y judicial en materia penal. Dentro de este segundo bloque, encontramos los siguientes organismos: el Sistema de Información de Schengen (SIS), el Sistema de Información Aduanera (SIA), Europol y Eurojust[84].

2. Análisis del Reglamento General de Protección de Datos

Este Reglamento se encarga de regular la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de los mismos. Con su entrada en vigor, deroga a la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos. El Reglamento surge a partir de la necesidad de cubrir los problemas que planteaba la directiva en lo referente a su falta de coherencia y de interpretación por parte de alguno de los Estados Miembros[85].

Teniendo esto en cuenta, es necesario destacar el considerando 13 del Reglamento ya que aborda la finalidad del mismo, así como lo que pretende proporcionar, y lo expresa de la siguiente manera[86]:

- "Para garantizar un nivel coherente de protección de las personas físicas en toda la Unión y evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior, es necesario un reglamento que proporcione seguridad jurídica y transparencia a los operadores económicos, incluidas las microempresas y las pequeñas y medianas empresas, y ofrezca a las personas físicas de todos los Estados miembros el mismo nivel de derechos y obligaciones exigibles y de responsabilidades para los responsables y encargados del tratamiento, con el fin de garantizar una supervisión coherente del tratamiento de datos personales y sanciones equivalentes en todos los Estados miembros, así como la cooperación efectiva entre las autoridades de control de los diferentes Estados miembros. El buen funcionamiento del mercado interior exige que la libre circulación de los datos personales en la

[84] ARENAS RAMIRO, M.: op. cit., pág 284
[85] REBOLLO DELGADO, L.: *Protección de datos en Europa: origen, evolución y regulación actual*, Ed. Dykinson, Madrid, 2018, pág 96.
[86] *Idem*, pág 97

> Unión no sea restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales[87]".

Para solucionar el problema de la homogeneidad, el legislador opta por variar el tipo normativo, al pasar de elaborar una Directiva a un Reglamento, esto lo que conlleva es a una eliminación de las variaciones o singularidades en el cumplimiento del núcleo de la materia por parte de los Estados Miembros, y, por lo tanto, aporta mayor inmediatez en lo que respecta a la consecución de sus finalidades, a la vez que establece un sustrato jurídico común para todos los Estados Miembros[88].

Otro rasgo destacable del Reglamento 679/2016, es que no es un texto cerrado, sino que contiene contenidos abiertos, esto significa que en muchas ocasiones remite a los Estados Miembros por medio de normas nacionales, a órganos de la Unión Europea (especialmente la Comisión Europea) del mismo modo, o utiliza conceptos jurídicos indeterminados o directrices adoptadas por las autoridades de control nacional[89].

Por último, la diferencia más significativa entre el Reglamento 679/29016 y la Directiva 95/46/CE es la concreción del término protección. La Directiva 95/46/CE dejaba la puerta abierta a vulneraciones de los derechos de los usuarios al fijar como contenido y elemento esencial la radicalización de los datos. El Reglamento 679/2016 palia esto al establecer como objetivo partir de la ubicación del interesado y donde se va a realizar dicha protección, esto se establece como elemento delimitador básico para aplicabilidad del mismo[90].

Su Considerando 2 deja ver el objetivo principal, el cual busca que "se contribuya a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo, a la convergencia de las economías dentro del mercado interior, así como el bienestar de las personas físicas.[91]"

[87] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016
[88] REBOLLO DELGADO, L. op. cit., pág 97
[89] *Idem*, pág 98
[90] *Idem, pág 99*
[91] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016

La titularidad del derecho se encuentra regulada en el art 1 del Reglamento y dice lo siguiente[92]:

- "1. El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos.
- 2. El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.
- 3. La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales."[93]

De este artículo lo que más destaca es su apartado 3, el cual hace referencia a uno de los principios fundacionales de la Unión Europea, el libre tránsito de personas y mercancías por todo el territorio, donde se incluye en esa libertad a los datos de carácter personal.
El artículo 2 trata el ámbito material, en su primer apartado, lo que destaca es la protección de las personas físicas debe ser tecnológicamente neutra, es decir es independiente del tratamiento utilizado, por lo que no cabe la distinción entre tratamientos automatizados y no automatizados. Su segundo apartado contempla aquellos casos en los que no sería de aplicación el Reglamento (como por ejemplo cuando se realizara por personas físicas, cuando las autoridades tuvieran fines de prevención, investigación, detención, enjuiciamiento, etc...)[94].

El concepto de datos personales no se ha visto modificado por el Reglamento, se sigue empleando la delimitación clásica la cual establece que toda la información sobre una persona física identificada o identificable. Una persona identificada o identificable no tienen el mismo significado, en este sentido, la primera acepción se refiere a los datos que de forma clara están vinculados con una persona y de los que se obtiene una información, es decir identifican al sujeto de forma directa. En cambio, el concepto de

[92] *Idem*, págs. 101 y 102
[93] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016.
[94]RODRÍGUEZ MUÑOZ J., "Disposiciones Generales. Título I (Arts.1-5 RGPD. Arts. 1.3 LOPDGDD)", en AA.VV. (CALVO LÓPEZ J.): *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, 2º ed., Ed. Wolters Kluwer, Madrid, 2019, págs. 326 y 327

identificable se emplea cuando la identidad de la persona pueda determinarse de forma directa o indirecta mediante un identificador[95].

Lo que introduce el Reglamento referido a este tema, es un nuevo concepto, la seudonimización, que se identifica con "aquellos datos que no pueden atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificable o identificada".[96]

Los principios relativos al tratamiento vienen regulados en el artículo 5. Lo interesante de este artículo, es que su fin, es la implicación en el resultado final de la norma, y da menos importancia al aspecto formal de la actividad del tratamiento y uso de los datos.[97]

El artículo 6 introduce uno de los principios más relevantes: el de licitud del tratamiento. Esta licitud solo puede tener su base en el consentimiento del sujeto titular del dato o bien en una norma de la Unión Europea o de los Estados Miembros. Este artículo introduce el concepto de interés legítimo, pero que necesita de una delimitación clara tanto por parte de la Unión Europea como de los Estados Miembros para evitar posibles vulneraciones del mismo. A pesar de que el reglamento en sí no detalla estos supuestos, podemos encontrar algunos ejemplos, como puede ser la prevención al fraude y la mercadotecnia directa, impedir atentados contra la seguridad de la red, entre otros[98].

El artículo 7 trata el consentimiento y las condiciones para el mismo. La Directiva 95/46/CE no exigía que el consentimiento fuera expreso, lo que conducía a que muchas veces el interesado marcara casillas o aceptara cosas que realmente no quería. Frente a esta situación de indefensión, lo que propone el Reglamento 679/2016 es que el

[95] REBOLLO DELGADO, L.: *Protección de datos en Europa: origen, evolución y regulación actual*, Ed. Dykinson, Madrid, 2018, pág 106
[96] *Idem*, pág 107
[97] *Idem*,.pág 108
[98] DÍAZ MARTOS N., "Principios (Arts.6-11 RGPD. Arts. 4-10 LOPDGDD)", en AA.VV. (CALVO LÓPEZ J.): *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, 2º ed., Ed. Wolters Kluwer, Madrid, 2019, págs. 333, 334 y 335.

consentimiento tenga que hacerse mediante un acto afirmativo que refleje la voluntad libre, el concepto de consentimiento queda perfectamente definido en al artículo 4.11 del Reglamento 679/2016[99].

Este artículo pone solución a la controversia con la información previa a la prestación del consentimiento, ya que recoge que hay que seguir el principio de transparencia, es decir que la información dirigida al público debe ser clara, concisa, accesible, y entendible por todo el mundo. En consecuencia, todas aquellas cláusulas que no cumplan estos requisitos no serán válidas a la hora de usar ese consentimiento.[100]

Los derechos del interesado se regulan en el Capítulo III del Reglamento 679/2016, que se centra esencialmente en el principio de transparencia. Este principio es la condición esencial para garantizar la protección de datos, porque asegura al interesado el derecho a saber y el derecho a decidir sobre el tratamiento de sus datos que realiza un tercero. Este principio tiene una categoría superior a la de los derechos de los interesados, al tratarlo como un principio del tratamiento de datos personales, esto lo que produce es que el responsable del tratamiento, realice el mismo conforme a este principio de forma continua, acreditando en todo momento que se está respetando la transparencia[101].

La efectividad de este principio está vinculada con el derecho de acceso a los datos personales (art 15), la rectificación (art.16), la supresión (art.1) y el derecho de oposición (art.21). El artículo 8 del Reglamento atiende sobre el principio de transparencia frente a menores, ya que los niños necesitan una protección específica[102].

Se pueden dar 2 momentos en los que el principio de transparencia se hace efectivo:

- El momento inicial que se corresponde con la asunción de capacidad de decisión sobre los datos de la persona por parte del responsable del tratamiento, este momento también se denomina como deber de información.

[99] *Idem*, pág 338
[100] *Idem*, pág 339.
[101] SALOM APARICIO J., "Derechos del interesado (Arts.12-19 RGPD. Arts. 11-16 LOPDGDD)", en AA.VV. (CALVO LÓPEZ J.): *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, 2º ed., Ed. Wolters Kluwer, Madrid, 2019, pág. 345
[102] *Idem*, pág 346

- La transparencia sobrevenida se da cuando una entidad que ya dispone y explota los datos de carácter personal (de forma legítima), prevé servirse de esa información para un objetivo adicional. Lo que implica este momento es, que la entidad deberá proporcionar al interesado toda la información necesaria sobre el cambio esencial en el tratamiento, al igual que proporcionarles información sobre las solicitudes de rectificación, supresión, oposición, etc…[103]

Este principio es un elemento que va a afectar a la totalidad del tratamiento de datos, en ningún momento se contempla su efectividad de forma parcial o a una parte concreta del tratamiento. Por último, cabe destacar que este principio no estaba consagrado en la Directiva 95/46/CE, por lo que el Reglamento 679/2016, de manera innovadora lo ha incorporado como un elemento clave para que haya lealtad y legitimidad en el tratamiento de datos.[104]

3. Instituciones y organismos de control

a. Organismos que establecen las garantías genéricas.

A. El Tribunal de Justicia de la Unión europea.

El Tribunal de Justicia de la Unión Europea (TJUE), cuenta con funciones jurisdiccionales, es decir[105], "es la instancia suprema cuya función es garantizar el respeto del Derecho Comunitario en la interpretación y aplicación de los Tratados[106]".

Respecto a su composición, se compone por un número de Jueces igual al número de Estados Miembros, y estos Jueces son asistidos por 8 Abogados Generales, ambos son elegidos por los Gobiernos de los Estados Miembros y nombrados por un período de seis meses, y su renovación se produce cada tres años[107].

[103] *Idem*, pág 347
[104] *Idem*, 348 y 349.
[105] ARENAS RAMIRO, M.: *El derecho fundamental a la protección de datos personales en Europa*, Ed. Tirant lo Blach, Valencia, 2006, pág 340
[106] TRATADO CONSTITUTIVO DE LA COMUNIDAD EUROPEA (artículo 220)
[107] ARENAS RAMIRO, M. *op. cit*., pág 340

Su labor se centra exclusivamente en "interpretar las disposiciones comunitarias, sin sustituir al órgano jurisdiccional nacional, y corresponde al Juez nacional, atendiéndose a esa interpretación, elegir la manera de adecuar el ordenamiento jurídico de su país a las exigencias de la legislación comunitaria[108]".

El tribunal tiene su regulación en primer lugar, en el artículo 19 del tratado de la Unión Europea, en segundo lugar, se desarrolla en el Tratado de Funcionamiento de la Unión Europea y, por último, el Protocolo 3 que tiene el estatuto del tribunal de justicia.

En materia de protección de datos destacan varias sentencias de este Tribunal. En primer lugar, la sentencia de 20 de mayo de 2003 (asunto Rechnungshof, (Austria)), donde el Tribunal de Justicia de la Unión Europea analiza si las cuestiones prejudiciales que enjuicia el Estado austriaco, cumplen los requisitos para la limitación del derecho fundamental a la protección de datos personales del artículo 8 del Convenio Europeo de Derechos Humanos, es decir, si existe una injerencia en el derecho, si persigue una finalidad legítima[109].

En segundo lugar, la sentencia de 6 de noviembre de 2003 (asunto Linqdvist), donde el Tribunal de Justicia de la Unión Europea se pronuncia por primera vez sobre el alcance del derecho de protección de datos en Internet. La sentencia trata sobre la publicación y difusión de datos sensibles en una página web lo que provocó el acceso a los mismos por un grupo indeterminado de personas. Lo relevante de esta sentencia es el pronunciamiento del Tribunal sobre la delimitación del concepto legal de datos personales, y sobre el concepto de datos relativos a la salud[110].

En tercer lugar, en su sentencia de 29 de enero de 2008, el Tribunal de Justicia de la Unión Europea, se centra en analizar el conflicto entre el derecho a la propiedad intelectual y los derechos a la intimidad y a la protección de datos personales, en relación con la confidencialidad en el ámbito de las comunicaciones electrónicas[111].

---

[108] STCE de 14 de octubre de 1999 (caso Adidas) (rec. núm. 1142/1998)
[109] GARRIGA DOMÍNGUEZ A.: *Nuevos retos para la protección de datos personales: en la era del Big Data y de la computación ubicua*, Ed. Dykinson, Madrid, 2016, pág 110
[110] Idem, pág 111
[111] Idem, pág 112

B. El Defensor del Pueblo Europeo

Este órgano está previsto en el Tratado de la Comunidad Europea. El Defensor del Pueblo está capacitado para recibir las reclamaciones por mala administración producidas por las instituciones u órganos comunitarios, de cualquier ciudadano de la Unión Europea, persona física o jurídica que tenga su domicilio social en un Estado Miembro. Por este motivo este órgano tiene una independencia total, por lo que sirve de intermediario entre el ciudadano y la Administración Comunitaria[112].

En materia de protección de datos destaca una carta escrita por este órgano al Presidente de la Comisión Europea donde se le solicita una clarificación de las normas comunitarias de protección de datos y propone cambios en las mismas[113].

b. Organismos que establecen las garantías específicas.

A. El Comité de Protección de Datos Personales

La Comisión de la Unión Europea recibe asistencia en sus competencias de ejecución por parte de distintos Comités con diferentes funciones. Para la materia de protección de datos se ha creado el Comité de Protección de Datos Personales. Lo integra el director de una autoridad de control de cada estado Miembro, por el Supervisor Europeo de Protección de Datos y por un representante de la Comisión, aunque no ostenta el derecho a voto. Se caracteriza por su actuación de manera independiente, al no poder recibir instrucciones de ningún organismo de la Unión europea. La nueva regulación introduce novedades en sus funciones, las cuales pueden realizar por iniciativa propia o a instancia de la Comisión. Se encuentran en el art.70 del Reglamento 679/2016.[114]

El Comité tiene la obligación de realizar un informe anual sobre la protección de las personas físicas en lo referente al tratamiento con la Unión Europea, al igual que con terceros países u organizaciones internacionales. Su contenido obligatorio consta de un

[112] ARENAS RAMIRO, M.: *El derecho fundamental a la protección de datos personales en Europa*, Ed. Tirant lo Blach, Valencia, 2006, pág 354
[113] *Idem*, pág 355
[114] *Idem*, pág 188

examen de la aplicación práctica de las directrices, recomendaciones y buenas practicas[115].

Los órganos establecidos en la Directiva 95/46/CE se ven sustituidos (en específico el G29), por uno nuevo (el Comité de Protección de Datos Personales), que crea el Reglamento General de Protección de Datos 679/2016. Este nuevo órgano, tiene un papel esencial en lo referente a la protección de datos en Europa junto con el Supervisor de Datos en Europa. Presenta personalidad jurídica y mayor carácter ejecutivo que el GT29. Su estructura es muy simple, consta de la figura del Presidente, dos Vicepresidentes y la secretaría que se desempeña por el Supervisor Europeo de Protección de Datos[116].

B. El Grupo de Protección (G29)

El G29 se corresponde con un grupo que crea la Comisión Europea, para que los ciudadanos pudieran acudir directamente a la Comisión ante posibles vulneraciones que se dieran en el tratamiento de sus datos personales en el ámbito comunitario. Es el Grupo de protección de las personas en lo que respecta al tratamiento de datos personales, es decir, es el intermediario entre las Autoridades de Control nacionales y la Comisión Europea[117].

Se compone por un representante de la Autoridad de Control designadas por cada Estado Miembro, por un representante de la Autoridad creada por las instituciones y organismos comunitarios y por un representante de la Comisión Europea. Este Grupo tiene un carácter consultivo e independiente, ya que las Autoridades que lo componen no están sujetas a ningún tipo de instrucción por parte de sus respectivos Gobiernos.
Algunas de las funciones que tiene asignadas el G29 son:

- Contribuir a la aplicación homogénea de las disposiciones nacionales que transporten las Directivas de Protección de Datos
- Asesorar e informar a la Comisión Europea sobre cualquier incidente en relación con la protección de datos personales

[115] *Idem*, pág 192
[116] *Idem*, pág 188
[117] ARENAS RAMIRO, M.: *El derecho fundamental a la protección de datos personales en Europa*, Ed. Tirant lo Blach, Valencia, 2006, pág 364

- Emitir Recomendaciones sobre cualquier asunto relacionado con el tratamiento de datos personales
- Emitir Dictámenes sobre los códigos de conducta comunitarios y sobre el nivel de protección de datos existente dentro de la Comunidad Europea y en los terceros países
- Y la función que más importancia tiene, emitir un Informe anual sobre la situación de la protección de las personas físicas en lo que respecta al tratamiento de datos personales en la Comunidad Europea y en los terceros países, el cual se da traslado al Parlamento Europeo, la Comisión Europea y al Consejo Europeo[118].

C. El Supervisor Europeo de Protección de Datos

Se crea bajo el mandato de la Unión Europea en 2004. El estatuto y las condiciones generales de ejercicio de las funciones del Supervisor se establecen en la Decisión nº1247/2002/CE del Parlamento Europeo, del Consejo Europeo y de la Comisión Europea, por otro lado, el Reglamento 679/ 2016, establece sus singularidades relativas a su actividad, en concreto las de coordinación con las autoridades nacionales de control[119].

La independencia que posee a la hora de ejercer su actividad es su característica más significativa. Su actividad principal gira en torno a la supervisión de la aplicación en las instituciones y organismos comunitarios los actos relativos a la protección de las personas físicas respecto al tratamiento de datos de carácter personal y la libre circulación de dichos datos (de conformidad con el art.6 del Tratado de la Unión Europea y del art.8 del Convenio Europeo de Derechos Humanos). El reglamento 45/2001 se encarga de recoger las condiciones de actuación y su estatuto. Así mismo, también establece el nombramiento, los recursos que dispone, la independencia, su obligación de secreto profesional, las funciones, sus competencias y las normas de procedimiento de su actuación[120].

[118] *Idem*, pág 365
[119] REBOLLO DELGADO, L.: *Protección de datos en Europa: origen, evolución y regulación actual*, Ed. Dykinson, Madrid, 2018, pág 194
[120] *Ibidem*

Sus competencias principales son el asesoramiento, la investigación y el control, en este sentido, tiene el derecho de acceso a datos personales, al igual que puede prohibir de forma temporal o definitiva un tratamiento de datos, también tiene legitimación de actuación en procesos relativos a la protección de datos ante el Tribunal de Justicia de la Unión Europea. Sus funciones pueden concretarse en:

- Conocer e investigar las reclamaciones que se le formulen.
- Asesorar organizaciones e instituciones comunitarias en materia de protección de datos.
- Mantener registros de los datos que se le notifiquen.
- Colaborar con las autoridades de control de los Estados Miembros y con las Autoridades Comunes de Control[121]

D. Las Autoridades Comunes de Control

Las Autoridades de Control de cada uno de los Estados Miembros tienen una serie de requisitos genéricos que se regulan mediante el Reglamento 679/2016. El Reglamento 679/2016 enfatiza la independencia que tienen en el desempeño de sus funciones y ejercicio de sus poderes sin en ningún caso, tener influencia externa (ya sea directa o indirecta), o recibir cualquier tipo de instrucción. Otro ámbito que destaca el Reglamento 679/2016 es que este órgano disponga de plena autonomía para regular a su personal y el presupuesto[122].

En los casos en que existieran varias autoridades de control debido al carácter territorial del Estado Miembro, este deberá decidir cuál de ellas representa al Estado en el Comité. En este órgano destaca la delimitación que hace el Reglamento entre sus funciones (recogidas en su art.57) y los poderes (establecidos en el art.58).[123]

E. El Grupo de Berlín

Surge por la iniciativa de la Autoridad de Protección de Datos de Berlín en 1983. Está compuesto por representantes de las Autoridades de Control de muchos Estados

[121] *Idem*, pág 195
[122] *Idem*, pág 196
[123] *Ibidem.*

Miembros, al igual que, por representantes de organizaciones internacionales públicas y privadas, y representantes de organizaciones internaciones industriales (todas de la Unión Europea)[124].

Tiene el objetivo de dar soluciones a los problemas que provocan las nuevas tecnologías y el uso de las telecomunicaciones en el derecho a la protección de datos personales, y plantean estas soluciones a través de Informes y Recomendaciones, por lo que su función es preventiva[125].

F. Autoridades Nacionales de Protección de Datos

La Directiva 95/46/CE regula tanto la necesidad de establecer autoridades de control de la protección de datos en los Estados Miembros, como también el establecimiento de principios y los criterios que se deben de seguir y la institución jurídica de estas instituciones en los países miembros. En el Considerando 63 de la Directiva 95/46/CE se establece que[126] "dicha autoridad debe disponer de los medios necesarios para cumplir su función, ya se trate de poderes de investigación o de intervención, tal autoridad ha de contribuir a la transparencia de los tratamientos de datos efectuados en el Estado Miembro del que dependa[127]". En España esta autoridad de control de identifica con la Agencia de Protección de Datos.

Las funciones de la Agencia de Protección de Datos se centran en dar respuesta a las necesidades de tutela, y en especial, al control en la protección de datos personales. Algunas de sus funciones son[128]:

- Controlar la aplicación del Reglamento General de Protección de Datos 2016/679 y, el resto de la normativa de protección de datos, así como proceder a que se aplique.

[124] ARENAS RAMIRO, M.: *El derecho fundamental a la protección de datos personales en Europa*, Ed. Tirant lo Blach, Valencia, 2006, pág 374
[125] *Ibidem*.
[126] HERRÁN ORTIZ, ANA I.: *El derecho a la intimidad en la nueva ley orgánica de protección de datos personales,* Ed. Dykinson, Madrid, 2002, pág 324
[127] Directiva 96/9/CE del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos
[128] HERRÁN ORTIZ, ANA I., *op. cit*. Pág 331

- Promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento. Las actividades dirigidas específicamente a personas menores de edad deberán ser objeto de especial atención.
- Asesorar, con arreglo al Derecho de los Estados miembros, al Parlamento nacional, al Gobierno y a otras instituciones y organismos sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento.
- Promover la sensibilización de las personas responsables y encargadas del tratamiento acerca de las obligaciones que les incumben en virtud del presente Reglamento 679/2016.
- Previa solicitud, facilitar información a cualquier interesado en relación con el ejercicio de sus derechos en virtud del presente Reglamento 679/2016 y, en su caso, cooperar a tal fin con las autoridades de control de otros Estados miembros.
- Tratar las reclamaciones presentadas por un interesado o por un organismo, organización o asociación de conformidad con el artículo 80 del Reglamento 679/2016, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable, en particular si fueran necesarias nuevas investigaciones o una coordinación más estrecha con otra autoridad de control.
- Cooperar, en particular compartiendo información, con otras autoridades de control y prestar asistencia mutua con el fin de garantizar la coherencia en la aplicación y ejecución del presente Reglamento 679/2016.
- Llevar a cabo investigaciones sobre la aplicación del presente Reglamento 679/2016, en particular basándose en información recibida de otra autoridad de control u otra autoridad pública.
- Hacer un seguimiento de cambios que sean de interés, en la medida en que tengan incidencia en la protección de datos personales, en particular el desarrollo de las tecnologías de la información y la comunicación y las prácticas comerciales.
- Fomentar la creación de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos con arreglo al artículo 42, apartado 1,

y aprobar los criterios de certificación de conformidad con el artículo 42, apartado 5 del Reglamento 679/2016.

- Llevar registros internos de las infracciones del presente Reglamento y de las medidas adoptadas de conformidad con el artículo 58, apartado 2 del Reglamento 679/2016.
- Desempeñar cualquier otra función relacionada con la protección de los datos personales[129].

c. El delegado de Protección de datos

El Delegado de Protección de Datos se considera como un "solucionador de cualquier situación relacionada con el tratamiento de datos personales que se le planteen por la dirección, terceros con los que se relacione su organización y por sus compañeros". Esta figura no resulta una completa novedad para todos los Estados Miembros, ya que algunos tenían figuras al desarrollar la Directiva 95/46/CE.

Ni el Reglamento 679/2016, ni la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales definen explícitamente a esta figura. Sin embargo, el Reglamento si introduce la figura de personas especializadas, por lo que tácitamente nos está definiendo al Delegado de Protección de Datos de la siguiente manera:

1. Introduce la necesidad de que tanto el encargado como el responsable de los datos cuenten con la ayuda de una persona especializada en la materia y en Derecho.
2. Tienen que poder desempeñar sus funciones de manera independiente.
3. Es necesario que sus conocimientos sean determinados.

Es importante destacar que el Delegado de Protección de Datos no es un sustituto de las Autoridades de Control, simplemente asegura el cumplimiento del Reglamento 679/2016 y de la normativa nacional, lo que sí ocurre, es una cooperación entre ambas, la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales establece

[129] Disponible en https://www.aepd.es/es/la-agencia/transparencia/informacion-de-caracter-institucional-organizativa-y-de-planificacion/funcion-y-poderes (fecha de última consulta 18 de mayo de 2021

que el delegado será el interlocutor de la Autoridad de Control. Es una figura que ayuda en la protección de datos y a su innovación[130].

Las funciones del delegado de Protección de Datos vienen estipuladas en primer lugar, en el art 39.1 del Reglamento, que dice lo siguiente:

- "El delegado de protección de datos tendrá como mínimo las siguientes funciones:
- a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;
- b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35.
- d) cooperar con la autoridad de control.
- e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto."[131]

y, en segundo lugar, de forma más concreta, en los arts. 36.1, 36.4 y 37 de la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales. Por último, esta figura se rige por los siguientes principios generales:

- Legalidad e integridad
- Profesionalidad

[130] ORS SANCHÉZ, C.: "El Delegado de Protección de Datos" en AA.VV. (CALVO LÓPEZ, J): *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, 1º ed., Ed.Wolters Kluwer. Madrid 2019, págs. 494-496.
[131] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016.

- Responsabilidad
- Imparcialidad
- Transparencia
- Confidencialidad

IV. LA PROTECCIÓN DE DATOS EN EL ÁMBTO SANITARIO. ESPECIAL INTERÉS EN SU TRATAMIENTO DEBIDO AL COVD-19.

La protección de datos es una materia que ha visto elevada su protección tanto los ordenamientos jurídicos nacionales como los internacionales. Dentro de esta, destacan la categoría de datos "sensibles", estos son aquellas cuestiones que guardan una mayor relación con el núcleo más interno de la personalidad y la dignidad humana. La particularidad de estos datos provoca que su utilización fraudulenta, tenga un carácter mayor de gravedad, y, en consecuencia, los distintos ordenamientos jurídicos se han visto obligados a reforzar su garantía y protección.

En España, la Ley Orgánica 15/1999 de 13 de diciembre regulaba este concepto de datos sensibles y los separaba en tres grupos o categorías. El primer grupo se corresponde con aquellas informaciones que revelaran datos sobre la ideología, afiliación sindical, religión y creencias. El segundo grupo se compone por aquellos datos relativos al origen racial, la salud y la vida sexual. El tercer grupo hace referencia a los datos de carácter personal relativos a la comisión de infracciones penales o administrativas. Nosotros nos vamos a centrar en el segundo grupo.[132]

El artículo 4 del Reglamento General de Protección de Datos contiene una serie de definiciones respecto a los principales conceptos que desarrolla el resto del articulado para que el análisis de las causas de legitimación y las obligaciones específicas sea

[132] DOMÍNGUEZ GARRIGA A., "La protección de los datos de carácter personal en el ámbito sanitario. Uso de la historia clínica.", en AA.VV. (GÓNZALEZ ÁLVAREZ S. y DOMÍNGUEZ GARRIGA A.: Dir.): *Historia clínica y protección de datos personales: especial referencia al registro obligatorio de los portadores del VIH*, 1º ed., Ed Dykinson, Madrid 2011, pág 15 y 16.

mucho más fácil. De este modo, el art.4.15 define a los datos relativos a la salud de la siguiente forma[133]:

- "datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud".[134]

Como se puede observar, este concepto incluye tanto los datos relacionados con la salud de la persona, como aquellos que incluyan información sobre el estado de la salud. El GT29 es el grupo de trabajo europeo independiente que se ha ocupado de cuestiones relacionadas con la protección de la privacidad y los datos personales, este determina que para que un dato se considere como un dato de salud debe de tener una de las siguientes características:

a. Datos inherentes o indiscutiblemente de carácter médico.
b. Datos en bruto de sensores que se pueden usar por si mismos o que al combinarlos con otros pueden inferir una conclusión respecto del estado de salud o el riesgo de salud de una persona (esto hace referencia a cualquier aparato tecnológico que establezca el número de pasos realizados, calorías ingeridas o consumidas, etc…).
c. Conclusiones inferidas sobre el estado o riesgo de salud de una persona.

El Reglamento también habla sobre datos genéticos y biométricos. Los primeros son considerados como una subcategoría dentro de los datos de salud, y quedan definidos en el art.4.13 de la siguiente forma[135]:

- "datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.[136]"

[133] RIGAUDIAS ÁLVAREZ C., "Tratamiento de datos de salud" en AA.VV. (MAÑAS PIÑAS J.L. Dir.): *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*, 1ª ed., Ed Reus S.A., Madrid 2016, pág. 165.
[134] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016
[135] RIGAUDIAS ÁLVAREZ C., *op.cit*., pág 174.
[136] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016

Los datos de salud contienen una protección reforzada por parte del Reglamento, el cual contempla que las causas de legitimación relacionadas con la prestación de asistencia sanitaria, el interés público, la investigación científica o histórica y con fines estadísticos, tienen que estar relacionadas con la existencia de una ley, ya sea de la Unión Europea o de un Estado Miembro.

En este sentido es necesario aclarar la interpretación de los conceptos de interés público, interés público en el área de la salud pública, interés vital, la investigación científica y los fines estadísticos.

En primer lugar, el sobre el interés público, el Reglamento establece que cuando se esté cumpliendo una obligación legal aplicable al responsable del tratamiento, si esta obligación es necesaria para el interés público, el tratamiento debe de tener una base en el Derecho de la Unión Europea o de los Estados Miembros, pero no sería necesario que cada tratamiento tuviera una normativa específica

En cambio, por interés público en el área de la salud pública se interpreta según lo establecido en el Reglamento 1338/2008 sobre estadísticas comunitarias de salud pública y de salud y seguridad en el trabajo, con aquellos elementos relacionados con la salud, en especial el estado de salud y la discapacidad. También se establece en relación con las necesidades de asistencia sanitaria, su acceso universal, los gastos y financiación de la misma y las causas de mortalidad. Resalta la necesidad de que este tipo de datos no sean tratados con otros fines por parte de terceros.

Por otro lado, la investigación científica debe entenderse como el tratamiento de datos personales con este fin, pero desde una asunción del concepto amplia, debido al art 179.1 del Tratado de Funcionamiento de la Unión Europea, el cual establece el objetivo de la Unión Europea de proporcionar un espacio europeo de investigación. Pero esto no quita las especialidades en lo referente a la publicación y comunicación de datos personales en el contexto de la investigación científica.

Dicha investigación científica tiene una causa de legitimación especifica regulada en el art.9 del Reglamento con dos elementos principales, en primer lugar, la existencia de una ley de la Unión Europea o de un Estado Miembro, y, en segundo lugar, que se cumplan las salvaguardas del art.89 del mismo[137]. Respecto al segundo elemento, sobre las salvaguardas, el Reglamento General de Protección de Datos, cuenta con unas muy específicas, que se pueden dividir en varios grupos.

El primero se corresponde con las salvaguardas éticas, que se resumen en las buenas prácticas clínicas, que son directrices elaboradas por los miembros de la Conferencia Internacional sobre Armonización de los requisitos técnicos para el registro de los medicamentos de uso humano (ICH) tomando como base los principios de la Declaración de Helsinki de la Asociación Médica Mundial. Esta salvaguarda se recoge en el Reglamento 536/2014.

El segundo grupo se corresponde con las salvaguardas técnicas, que se identifican con la minimización de los datos personales y la seudonimización.[138]

Estas técnicas de anonimización que se encuentran reguladas en el art.89 del Reglamento, se aplicarán siempre que no afecten a los fines de la investigación. Hay dos tipos de anonimización, el primero se corresponde con la anonimización absoluta la cual no es exigible por el Reglamento debido a que su realización no es posible según las reglas de la buena fe clínica y por otro lado destruiría el valor científico del dato.[139]

En segundo lugar, la técnica de anonimización parcial es la seudoanonimización, que el Reglamento define de la siguiente forma:

- "el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas

[137] RIGAUDIAS ÁLVAREZ C., *op.cit*., págs. 175, 176 y 177
[138] *Idem* pág 179.
[139] RIGAUDIAS ÁLVAREZ C.: Tratamiento de datos con fines de investigación científica y/o médica en AA.VV. (LOMBARTE RALLO A. Dir.): *Tratado de Protección de Datos*, 1ª ed., Ed. Tirant Lo Blanch, 2019, págs. 729, 730 y 731.

> destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable."

El Reglamento establece a la seudoanonimización como una medida de seguridad, por lo que no necesita una causa de legitimación propia, como si sucedía con la Directiva 95/96/CE. También los datos seudoanonimizados se siguen reconociendo como datos personales, al establecer el reglamento en su considerando 26 que dichos datos "deben considerarse información sobre una persona física identificable".

La seudoanonimización es un estándar obligatorio tanto en los ensayos clínicos de la Unión Europea como en muchas otras regiones del mundo, debido a que dificulta la posible identificación de aquellos pacientes que intervienen en la misma.[140]

Dentro de este grupo de salvaguardas técnicas también se encuentra la codificación, que es el método que debe emplearse en los estudios clínicos. La principal diferencia con la seudoanonimización es que la codificación se debe realizar por el investigador principal por mandato de la ley.

El tercer grupo, se corresponde con las salvaguardas legales y contractuales que se identifican con aquellas relaciones contractuales que se establecen entre laboratorios, centros investigadores etc… Estas relaciones se regulan por sus requisitos regulatorios propios y el art.28 del Reglamento.

El cuarto grupo se corresponde con las salvaguardas estatutarias que básicamente es el deber estatutario de confidencialidad de los profesionales sanitarios, regulado por el Código de deontología médica del Consejo General de Colegios Oficiales de Médicos de España.

Y el último grupo se corresponde con las salvaguardas del Reglamento que son unas obligaciones adicionales que se deben de tener en cuenta a la hora de realizar la investigación.[141]

[140] RIGAUDIAS ÁLVAREZ C., 2016, *op.cit*., págs. 180 y 181.

Otro tema a tratar es la compatibilización de distintos tratamientos. Tras haber establecido que unos datos personales se corresponden con una causa de legitimación en concreto, si se quiere usar otro tratamiento con un fin distinto al inicial, es necesario pasar un test de compatibilidad, si no se superara este test, el procedimiento a seguir sería volver a establecer una causa diferente de legitimación según el art.9 del Reglamento.[142]

El consentimiento de los interesados cuando la causa de legitimación del tratamiento de datos de salud es la investigación científica debe interpretarse desde un sentido amplio, esto quiere decir que el consentimiento no solo cubre el objeto del ensayo clínico, sino que además se incluyen posibles fines de investigación más amplios, es decir, cubre la finalidad completa de ese proyecto o investigación.[143]

Dentro del consentimiento es necesario diferenciar entre el que establece el Reglamento General de Protección de Datos y el del Reglamento 536/2014. El consentimiento del RGPD se interpreta de forma amplia como se comentó anteriormente, en cambio el del Reglamento 536/2014 se basa en la participación en el ensayo clínico, no entraría por lo tanto el tratamiento de datos, ya que esa materia la trata el Reglamento General de Protección de Datos.[144]

Las obligaciones específicas del tratamiento de datos de salud que se establecen en el Reglamento General de Protección de Datos, se centran principalmente en el tratamiento a "gran escala", no tiene una definición como tal dentro de esta normativa, pero en su considerando 91 se establece una definición del concepto, al igual que contempla aquellos tratamientos que no se corresponden con el referido a gran escala.

[141] RIGAUDIAS ÁLVAREZ C., 2019, *op.cit*., págs. 732, 733, 734 y 735.
[142] RIGAUDIAS ÁLVAREZ C., 2016, *op.cit*., pág 182.
[143] *Idem* pág 183.
[144] RIGAUDIAS ÁLVAREZ C.: Tratamiento de datos con fines de investigación científica y/o médica en AA.VV. (LOMBARTE RALLO A. Dir.): *Tratado de Protección de Datos*, 1ª ed., Ed. Tirant Lo Blanch, 2019, págs. 723 y 724.

Teniendo esto es cuenta, se puede concretar que el tratamiento de datos a gran escala se corresponde con tratar una cantidad de datos personales a nivel regional, nacional o supranacional que podrían afectar a un gran número de afectos y que entrañen un alto riesgo por razones de sensibilidad. En este grupo no se pueden incluir aquellos datos personales cuyo tratamiento lo realice un solo médico u otro profesional de la salud o abogado.

El tratamiento a gran escala establece una serie de directrices:

1. Nombrar un representante en el caso de responsables y encargados no establecidos en la UE y sujetos al Reglamento.
2. Nombrar un Delegado de Protección de Datos en el sector privado.
3. Llevas una evaluación de impacto relativa a la protección de datos donde se trate si este tipo de tratamiento supone un alto riesgo para los derechos y libertades fundamentales de las personas físicas.
4. Llevar a cabo una consulta previa a la autoridad de control.[145]

Los datos contenidos en los ensayos clínicos se pueden transferir a los siguientes destinatarios fuera del Espacio Económico Europeo:

- Cuando el promotor estuviera establecido fuera del Espacio Económico Europeo.
- Entidades del grupo promotor que estuvieran establecidas fuera del Espacio Económico Europeo.
- Entidades públicas con competencias en materia de salud fuera del Espacio Económico Europeo.
- Colaboradores científicos establecidos fuera del Espacio Económico Europeo.

Cuando los datos se corresponden con información de los pacientes, estos deben de estar codificados siguiendo las distintas finalidades para cada uno de los supuestos anteriormente mencionados. En cambio, si los datos se corresponden con los datos de

[145] RIGAUDIAS ÁLVAREZ C., 2016, *op.cit* 183 y 184.

los investigadores y su equipo, estas transferencias de datos solo se harán si es necesario para una lista cerrada de finalidades.[146]

V. ACTUALIZACIONES PRODUCIDAS POR LA COVID-19.

El estado actual en el que nos encontramos debido a la pandemia producida por la Covid-19 ha planteado retos en todos los ámbitos, como la economía, la política, en lo social, pero especialmente ha sido un reto a nivel jurídico. Los derechos fundamentales y la vulneración de los mismos ha sido uno de los temas centrales durante este periodo. Los más controversiales han sido aquellos que se han podido ver afectados por la aplicación de algún Decreto-ley, como puede ser el derecho a la libre circulación, a la intimidad, la libertad de expresión y la protección de datos de carácter personal.

El derecho a la protección de datos que está íntimamente ligado al derecho a la intimidad se encuentra en una batalla contra el interés público y la defensa de la salud pública. Esto se debe, a que, debido a la pandemia, ha habido una avalancha de "intentos" de ayudar a controlar la propagación del virus mediante el desarrollo de aplicaciones móviles de geolocalización, las cuales en "teoría" avisan cuando hay cerca un posible positivo, o detectan aquellas personas que han estado en contacto con un positivo, o aplicaciones de autoevaluación de salud o las técnicas de mapeo de contactos, todas ellas con la finalidad de ayudar a disminuir los casos y los contagios.

Las cuestiones sobre la afectación de la privacidad se reflejan sobre las medidas adoptadas por el Gobierno en la OSND/297/2020, de 27 marzo, por la que se encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de diversas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19.

Pero, ¿es esta situación de excepcionalidad razón suficiente para incidir sobre el flujo y la exposición de nuestros datos? ¿tiene la defensa de la salud pública mayor preponderancia frente a la protección de nuestros datos?

[146], RIGAUDIAS ÁLVAREZ C., 2019, *op.cit* págs. 714 y 715.

Antes de responder a estas preguntas es necesario recordar que la normativa referente a la protección de datos se despliega cuando efectivamente estemos ante datos personales. Esto quiere decir, que dichos datos o información identifique o haga identificable a cualquier sujeto (esto es el concepto amplio que utiliza el Reglamento General de Protección de Datos y el Tribunal de Justicia de la Unión Europea). Pero esa susceptibilidad de identificación no debe de resultar difícil o necesitar de operaciones complejas para su obtención. El Tribunal de Justicia de la Unión Europea ha reafirmado en varias ocasiones que el presupuesto de identificabilidad no es solo la recopilación y tratamiento de los datos, sino que también interviene el ejercicio por parte del interesado (haciendo referencia al derecho al olvido, rectificación, etc…).

Se puede hacer una división de los datos según sean individualizados, seudonimizados o anónimos. Los dos primeros grupos son los que supondrían una vulneración del derecho, es por esto, que estarán sometidos a las cautelas y garantías de la normativa de protección de datos, a través de un acceso y un tratamiento lícito, leal y transparente, cuya finalidad es limitada y, respetando los parámetros de proporcionalidad, adecuación, pertinencia y limitación, al igual que el principio de exactitud de los datos o principio de calidad, y su conservación limitada. Los datos anónimos por su parte no representan ningún tipo de peligro debido a su naturaleza.

Los datos sensibles son aquellos datos de carácter personal cuya recopilación o tratamiento afecta de forma más intensa a otros derechos fundamentales relacionados, por lo que, a dichos datos, tanto el Reglamento General de Protección de Datos, como la Ley Orgánica Protección de Datos y Garantía de los Derechos Digitales le proporcionan una protección específica. Los datos sensibles se corresponden con la ideología, identidad u orientación sexual, creencias, y todo lo referente al estado de salud (es decir, tanto salud física como psíquica).

Las aplicaciones móviles de geolocalización consisten en permitir conocer una ubicación concreta. Esta no tiene porqué vulnerar la privacidad o la capacidad de disposición de nuestros datos, ya que existe una modalidad anónima, pero la que afecta

se corresponde con la que permite la identificación del individuo de forma directa o indirecta.

La geolocalización que puede suponer un problema es la que identifica al usuario de forma indirecta, es decir aquella que no dispone de anonimización. Esta, sin embargo, se puede justificar desde que el usuario aporta su consentimiento para la utilización de la misma, al igual que mediante alguno de los supuestos de tratamiento lícito previstos en la normativa de protección de datos, es decir, la garantía de la salud pública y el freno de la pandemia.

Los usos sociales, por lo tanto, es lo que limita a los derechos fundamentales como la privacidad, intimidad u honor, ya que es el propio individuo el que expone y proporciona a terceros datos como su orientación sexual, los gustos personales, el perfil económico, visión política etc… Es decir, los usuarios perciben que el valor añadido que les proporcionan las aplicaciones móviles prima sobre la exposición de datos sensibles.

Por este motivo, es necesario señalar la excepción prevista en el art.9.2 del Reglamento General de Protección de Datos que establece la prohibición de tratamiento en los casos que dichos datos personales se hayan hecho manifiestamente públicos por el interesado. Por lo tanto, para delinear la privacidad, es necesario que la información sobre los datos personales que se tratan, al igual que cómo se tratan, dónde se almacenan y durante cuánto tiempo, le sea facilitada al usuario de forma directa, precisa y clara o inteligible.

Por otro lado, las aplicaciones móviles de autoevaluación de salud y de información sanitaria, tienen varios objetivos, en primer lugar, el autodiagnóstico de la Covid-19, y, en segundo lugar, acceder a la información pública actualizada por las autoridades sanitarias. Estas aplicaciones móviles han sido desarrolladas por la Orden de la Secretaría de Estado de Digitalización e Inteligencia Artificial que además permiten la geolocalización del usuario sólo en aquellos casos en que este otorgue su consentimiento explícito a fin de poder prestar el servicio de emergencia.

La finalidad de la recopilación de datos se centra en controlar la propagación del virus, por lo que reviste un fuerte interés público. Hay que tener en cuenta, que este tipo de aplicaciones móviles inciden directamente sobre la categoría de datos sensibles que comentamos anteriormente, y que, por lo tanto, a priori se podría asegurar que su uso es inapropiado, pero el acceso a estas aplicaciones móviles cumple los requisitos que exige la normativa de protección de datos, ya que no sólo se cuenta con el consentimiento del usuario, sino que además ese acceso está justificado por una finalidad de interés público. Esto está expresamente previsto tanto en la legislación de protección de datos, como en la legislación de sanidad que se corresponde con la Ley 3/1986, de 14 de abril, o la Ley 33/2011, de 4 de octubre, General de Salud Pública.

Quizás lo único que no pueden asegurar tanto la geolocalización como la autoevaluación de salud es el uso secundario de los datos, por lo que no se puede garantizar con total seguridad que los datos personales, especialmente los denominados sensibles no vayan a circular o a utilizarse de formas distintas a las que el individuo tenía pensadas.

Tras lo expuesto, queda claro que tanto las aplicaciones de geolocalización como las de autoevaluación de salud, cumplen con las garantías necesarias para la protección de datos de carácter personal. En ambas se cumple el consentimiento y la voluntariedad del sujeto, y tienen un interés público debido a la situación actual[147].

La Unión Europea junto con los Estados Miembros, también han trabajado juntos apoyando el desarrollo de aplicaciones móviles, más concretamente las de rastreo, las cuales tienen como finalidad advertir a aquellas personas que hayan podido estar en contacto con algún positivo por Covid-19, sin olvidar la importancia de garantizar que estas aplicaciones móviles respeten la privacidad y la protección de datos, pero sin perder su eficacia.

[147] HERRERO TIMÓN M.: *Protección de datos de carácter personal y crisis sanitaria (Covid 19)*, 2020, disponible en https://elderecho.com/proteccion-de-datos-de-caracter-personal-y-crisis-sanitaria-covid-19 (última consulta 15 de mayo de 2021)

En este sentido, el Parlamento resaltó su preocupación sobre la garantía del derecho a la privacidad y a la protección de datos, es por esto que en su resolución del 17 de abril de 2020 (citar la sentencia) comenta que cualquier medida digital contra la pandemia (incluimos en las mismas las aplicaciones móviles) debe respetar plenamente la legislación en materia de protección de datos y privacidad, y añade, que el uso de dichas aplicaciones no ostentará carácter obligatorio y contarán con cláusulas de cancelación para que su uso concluya una vez finalizada la pandemia.

Por otro lado, los eurodiputados subrayaron la necesidad de la anonimidad de los datos, al igual que estos no deberían ser almacenados en bases de datos centralizadas para evitar posibles abusos o intrusiones en los mismos. También pone de manifiesto la importancia de señalar como estas aplicaciones móviles de rastreo van a ayudar a minimizar las tasas de contagios, y como se ejecutarán los intereses comerciales de los desarrolladores.

Las aplicaciones móviles de rastreo en la Unión Europea son aplicaciones basadas en la geolocalización, es decir, aplicaciones que recogen datos en tiempo real sobre la ubicación precisa y movimientos de las personas, al igual que recopilan información sobre la salud. Estas aplicaciones, por lo tanto, pueden avisar a los usuarios que han estado cerca de una persona infectada por un tiempo determinado. El funcionamiento de estas aplicaciones permitiría rastrear y supervisar los contagios, estableciendo una mayor precisión y una limitación a la propagación, pero aumentarían considerablemente el riesgo para la privacidad y la protección de datos de los individuos.

Para minimizar los riesgos y limitar la intrusión, la Comisión Europea junto con los Estados Miembros, el Supervisor Europeo de Protección de Datos y la Junta Europea de Protección de Datos han desarrollado una serie de directrices y medidas para el desarrollo de las aplicaciones relacionadas con la Covid-19 (en concreto las Directrices 04/2020 sobre el uso de datos de geolocalización y herramientas de rastreo de contactos en el contexto de la pandemia, y las Directrices 03/2020 sobre el tratamiento de datos relativos a la salud con fines de investigación científica en el contexto del brote de COVID-19) , las cuales tienen como base el pleno respeto a las normas de protección de

datos, en particular, el Reglamento General de Protección de Datos, y la directiva de privacidad electrónica.

Las medidas establecidas son las siguientes:

- Las autoridades sanitarias nacionales deberían aprobar las aplicaciones y ser responsables del cumplimiento de las normas de protección de datos personales de la UE.
- Los usuarios mantienen el control total de los datos personales. La instalación de la aplicación debe ser voluntaria y debe desmontarse tan pronto como ya no sea necesaria.
- Limita el uso de datos personales: solo datos relevantes para el propósito en cuestión, y no debe incluir el seguimiento de la ubicación.
- Límites estrictos en el almacenamiento de datos: los datos personales no deben conservarse más tiempo del necesario.
- Seguridad de los datos: los datos deben almacenarse en el dispositivo de un individuo y encriptarse.
- Interoperabilidad: las aplicaciones deberían ser utilizables a través de las fronteras de la UE.
- Las autoridades nacionales de protección de datos deben involucrarse y consultarse por completo.

Por último, la Comisión señaló que el uso de estas aplicaciones de rastreo y de geolocalización deben ser interoperables, es decir, que las personas puedan usarlas para recibir alertas en cualquier lugar de Europa en el que se encuentren.

El 13 de mayo de 2020, la Comisión incluyó el uso de aplicaciones de rastreo de contactos entre las pautas para reanudar los viajes en Europa y señaló que tienen que ser interoperables para que las personas puedan usarlas para recibir alertas en cualquier lugar de Europa en el que se encuentren.

Ciertamente lo único que se debe mejorar a la hora de utilizar estas aplicaciones móviles es la forma en la que se traten los datos, ya que es necesario que se respeten los principios generales de calidad y minimización de los datos; garantizando que la

duración del tratamiento y la conservación de datos sea la estrictamente necesaria para el cumplimiento de la finalidad definida[148].

VI. CONCLUSIONES.

A la vista de lo expuesto en los apartados anteriores, se pueden obtener las siguientes conclusiones:

En primer lugar, que la protección de datos es un derecho que es relativamente nuevo, debido a que empezó a surgir su necesidad a medida que iba avanzando la tecnología. También es curioso ver como al principio, la protección de datos se usaba en lo referente a conflictos bélicos, después cambió a ser un derecho de los usuarios frente al poder público, hasta convertirse en un requisito necesario prácticamente para cualquier actividad que se realice en el día a día.

Por otra parte, es curioso ver la evolución de los derechos fundamentales a lo largo del tiempo y como estos van cambiando en función de la sociedad del momento. La inclusión del derecho a la protección de datos a este grupo, desde mi punto de vista era algo necesario, ya que actualmente cuando se vulnera o se infringe la protección de los datos personales de un individuo, realmente es como si alguien externo tuviera acceso a cualquier ámbito de tu vida, personal, laboral, familiar, en este sentido una infracción del mismo implica además una vulneración en otros derechos, como puede ser el derecho a la intimidad, privacidad, etc…

En consonancia con esto, la evolución normativa también ha tenido un avance significativo, siendo cada vez más precisa y llevando a cabo diferentes medidas, donde cada una de ellas tiene como fin, en primer lugar, garantizar y proteger a los individuos de posibles vulneraciones del derecho de protección de datos, y en segundo lugar, una vez protegidos los datos, su correcto tratamiento, y para llevar a cabo esto, crea figuras como la del Delegado de Protección de Datos, o instituciones u órganos como el Comité

[148] Disponible en www.europarl.europa.eu/news/es/headlines/priorities/respuesta-de-la-ue-ante-el-coronavirus/20200429STO78174/apps-contra-el-covid-19-como-garantizar (última consulta 15 de mayo de 2021)

de Expertos para la Protección de Datos, el Comité Consultivo, las Autoridades de Control, etc…

Por último, se ha tratado el tema de la protección de datos en el ámbito sanitario, dándole especial importancia a los datos denominados como sensibles, viendo sus particularidades y requisitos especiales que plantea el RGPD. De igual modo, se ha visto como la incidencia del COVID-19 ha creado controversia entre el derecho a la protección de datos y el interés público sanitario producido por esta pandemia.

Está claro que la protección de datos es un derecho que va a seguir desarrollándose con el paso del tiempo, y que las aplicaciones empleadas para ayudar a superar esta pandemia siguen los requisitos estipulados en la normativa, pero finalmente será el tratamiento que se emplee en los datos lo que podrá provocar una vulneración de los derechos fundamentales, y estas consecuencias secundarias es algo que actualmente es complicado de apreciar y regular correctamente.

VII. BIBLIOGRAFÍA.

CAMPUZANO TOMÉ, H.: *Vida privada y datos personales,* Tecnos, Madrid, 2000

CONDE ORTIZ, C.: *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad*, Ed. Dykinson, Madrid, 2006.

DENNINGER, E.: *El derecho a la autodeterminación informativa*, en PÉREZ LUÑO, ANTONIO E.: *Problemas actuales de documentación y la informática jurídica*, Tecnos Madrid

DÍAZ MARTOS N., "Principios (Arts.6-11 RGPD. Arts. 4-10 LOPDGDD)", en AA.VV. (CALVO LÓPEZ J.): *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, 2º ed., Ed. Wolters Kluwer, Madrid, 2019

DOMÍNGUEZ GARRIGA A., "La protección de los datos de carácter personal en el ámbito sanitario. Uso de la historia clínica.", en AA.VV. (GÓNZALEZ ÁLVAREZ S. y

DOMÍNGUEZ GARRIGA A.: Dir.): *Historia clínica y protección de datos personales: especial referencia al registro obligatorio de los portadores del VIH*, 1º ed., Ed Dykinson, Madrid 2011.

FREIXAS GUTIERREZ, G.: *La protección de los datos de carácter personal en el derecho español*, Bosh, Barcelona

FROSINI, V: *Bases de datos y tutela de la persona*. Revista de Estudios Políticos (NE) nº 30 de 1982

FROSINI, V.: *Informática y Derecho*, Ed. Temis, 1988

GARRIGA DOMÍNGUEZ A.: *Nuevos retos para la protección de datos personales: en la era del Big Data y de la computación ubicua*, Ed. Dykinson, Madrid, 2016

HERRÁN ORTIZ, ANA I.: *El derecho a la intimidad en la nueva ley orgánica de protección de datos personales,* Ed. Dykinson, Madrid, 2002

MADRID CONESA, F: *Derecho a la intimidad, informática y Estado de Derecho*. Universidad de Valencia. Valencia 1984

ORS SANCHÉZ, C.: "El Delegado de Protección de Datos" en AA.VV. (CALVO LÓPEZ, J): *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, 1º ed., Ed.Wolters Kluwer. Madrid 2019.

ORTIZ HERRÁN, ISABEL A.: *El Derecho a la Intimidad en la nueva Ley Orgánica de Protección de Datos Personales*, Ed. Dykinson, Madrid, 2002.

PÉREZ LUÑO, ANTONIO E.: "*Del habeas corpus al habeas data",* en Informática y Derecho, nº 1, UNED, Centro Regional de Extremadura, Mérida

PÉREZ-LUÑO, A.: "Nuevos derechos fundamentales de la era tecnológica: la libertad informática", *ADPEP*, núm.2 1989/90

RAMIRO ARENAS, M.: *El Derecho fundamental a la protección de datos personales en Europa*, Ed. Tirant lo Blanch, Valencia ,2006

REBOLLO DELGADO, L.: *Protección de datos en Europa: origen, evolución y regulación actual*, Ed. Dykinson, Madrid, 2018.

REBOLLO DELGADO, L.: *Introducción a la protección de datos*, Ed. Dykinson, Madrid, 2008.

RIGAUDIAS ÁLVAREZ C., "Tratamiento de datos de salud" en AA.VV. (MAÑAS PIÑAS J.L. Dir.): *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*, 1ª ed., Ed Reus S.A., Madrid 2016.

RIGAUDIAS ÁLVAREZ C.: Tratamiento de datos con fines de investigación científica y/o médica en AA.VV. (LOMBARTE RALLO A. Dir.): *Tratado de Protección de Datos*, 1ª ed., Ed. Tirant Lo Blanch, 2019

RODRÍGUEZ MUÑOZ J., "Disposiciones Generales. Título I (Arts.1-5 RGPD. Arts. 1.3 LOPDGDD)", en AA.VV. (CALVO LÓPEZ J.): *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, 2º ed., Ed. Wolters Kluwer, Madrid, 2019

SALOM APARICIO J., "Derechos del interesado (Arts.12-19 RGPD. Arts. 11-16 LOPDGDD)", en AA.VV. (CALVO LÓPEZ J.): *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, 2º ed., Ed. Wolters Kluwer, Madrid, 2019.

WESTIN, ALAN F.: *Privacy and Freedom, Atheneum*, 25 Wash. & Lee L., 1970